Microsoft

Microsoft Windows 2000 Server

Operating System

Mapping Certificates to User Accounts

Beta 3 Technical Walkthrough

Abstract

The Microsoft® Windows® 2000 operating system provides a very rich administrative model for managing user accounts. In a corporate environment with relatively few threats, the user account/password model works very well. However, the situation changes on the Internet. The Internet is a very hostile environment and user ID/password attacks that are impractical in a corporation are possible. Certificate mapping provides an elegant solution to this situation by using public-key technology that is much harder to attack than password-based systems. In Windows 2000, it is possible to map a certificate that has been issued to a user to the user's account. A server application can then use public-key technology to authenticate the user through this certificate. If the user is authenticated, the user's account is logged on. The result is the same as if user had provided a user ID and password; yet the process is much more secure. This walkthrough demonstrates how to map public-key certificates to a Windows 2000 user account so that it can be used with Internet Information Server (IIS).

THIS IS PRELIMINARY DOCUMENTATION. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This BETA document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0599

CONTENTS

INTRODUCTION

Traditionally, computer systems have used a centralized accounts database to manage users, their privileges, and their access controls. This technique has worked well and is well understood. However, as systems become more and more distributed—with hundreds of thousands to millions of users—this form of centralized control becomes unwieldy. The problems range from trying to verify an account against a database located across the Internet, to administering a lengthy list of users.

Public key certificates have the potential to help simplify these problems. Certificates can be widely distributed, issued by numerous parties, and verified by examining the certificate without having to refer to a centralized database. However, existing operating systems and administration tools can only deal with accounts, not certificates. The simple solution—one that maintains the advantages of both certificates and user accounts—is to create an association (or *mapping*) between a certificate and a user account. This allows the operating system to continue using accounts while the larger system and the user use certificates.

In this model, a user presents a certificate, and the system looks at the mapping to determine which user account should be logged on. This should not be confused with smart card logons. Microsoft® Windows® 2000 supports smart card logon, and that mapping is implicit. For more information, see the Windows 2000 Beta 3 walkthrough on smart card logon.

Mapping a certificate to a Windows 2000 user can be done either by the Windows 2000 Active Directory™ directory service or with rules defined in Microsoft 2000 Internet Information Service (IIS). This walkthrough will help you map public key certificates to a specific Windows 2000 user account. The certificate can then be used to authenticate the user with a Windows 2000 computer running Internet Information Service.

TYPES OF MAPPING

In most cases, a certificate is mapped to a user account in one of two ways: a single certificate is mapped to a single user account (one-to-one mapping), or multiple certificates are mapped to one user account (many-to-one mapping).

User Principal Name Mapping

User principle name mapping is a special case of one-to-one mapping. User principal name mapping is only available through the Active Directory. Enterprise certificate authorities (CAs) place an entry, called a UPN, into each certificate. The UPN looks very much like an e-mail name. The UPN is unique within a Windows 2000 domain. The UPN is used to find the user's account in the Active Directory, and that account is logged on. UPN mappings are implicit in Windows 2000, and this is the method used by smart card logon. See the next section on Active Directory mapping for more details.

One to One

One-to-one mapping is the mapping of a single user certificate to a single Windows 2000 user account. For example, assume that you want to provide a Web page to your employees that will allow them to view and modify their deductions, manage their health care, and a number of other benefits options. You want this page to work over the Internet, and you need it to be secure. As a solution, you decide to use Windows 2000, certificates, and certificate mapping. You can either issue certificates to each of your employees from your own certificate service, or you can have your employees obtain certificates from a CA approved by your company. You then take these user certificates and map them to the employees' Windows 2000 user accounts. This allows a user to connect to the Web page, using the Secure Socket Layer (SSL) from anywhere by providing his or her client certificate. The user logs on using his or her own user account, and normal access controls can be applied.

Many to One

Many-to-one mapping is the mapping of many certificates to a single user account. For example, assume that you have a partnership with an agency that provides temporary workers for your job openings. You would like to allow the agency personnel to view Web pages describing current job openings that are otherwise accessible only to company employees. The agency has its own CA that it uses to issue a certificate to its employees. After installing the agency CA's root certificate as a trusted root in your enterprise, you can set a rule that maps all certificates issued by that CA to map to a single Windows 2000 account. You then set access rights so that this account can access the Web page. Typically, you give the user account the same name as the agency.

When temporary employees from the agency connect to the agency's Web server and provide their certificates, they are mapped to the same account and can access the Web page. However they cannot view other pages since the account does not have permissions to anything else. This is nice from an administrative viewpoint because the agency can now issue certificates and manage its users without requiring further intervention on your part.

WHERE MAPPING OCCURS

With IIS in Windows 2000, the certificate mapping can take place in one of two places. Either IIS or the Active Directory can map the certificate to a Windows 2000 user.

IIS

When IIS does the mapping, the certificate is compared to a list of rules that IIS maintains in its metabase. IIS finds a rule that matches the indicated Windows 2000 account. IIS mapping is configured for each Web server and is useful if you need very few mappings or a different mapping on each Web server. Most customers will prefer to use the Active Directory mapping since it requires less administration.

Active Directory

In Active Directory mapping, when the IIS server receives a certificate from the user, it passes it on to the Active Directory, which maps it to a Windows 2000 user account. The IIS server then logs this account on.

Active directory mapping is most useful when the account mappings are the same on all IIS servers. Administration is simplified since the mapping is done in only one place.

Mapping in the active directory can happen in one of two ways. The administrator can explicitly map a certificate to a users account. This certificate can come from any source, as long as the root CA for that certificate is trusted for client authentication.

UPN mapping can also be used. A UPN is automatically put into a certificate issued by an enterprise CA. If a certificate is passed to the Active Directory for mapping, it is first examined for UPN mapping. Only if UPN mapping is not possible is the mapping set by the administrator used.

UPNs are in the form of *userid@domain*. If the certificate contains a UPN, the domain is within the hierarchy of the directory, and the CA that issued the certificate is trusted to put UPNs in the certificate, the user’s account is retrieved from the directory and logged on. All these conditions must be true before the user’s account is retrieved. If any of these conditions is false, the directory is searched for a mapping set by the administrator.

REQUIREMENTS

Prior to using this walkthrough, see the release notes for information that may have changed since this paper was written.

This walkthrough requires the following:

- Windows 2000 Beta 3 RC0 or later.
- A trusted certificate authority
- A user certificate service or certificates issued by a trusted CA
- A Windows 2000 Active Directory
- Internet Information Service
- Administrative permissions

GETTING THE USER CERTIFICATE

Requesting a User Certificate

For this walkthrough you will need to request a user certificate. If you wish to use UPN mapping, you should get a certificate from an enterprise CA in your domain. However, for all other mapping methods, you should use a certificate from a CA that is not in your enterprise. This ensures that UPN mapping is not occurring when you test the mapping at the end of this walkthrough. For more details, see the walkthrough documents entitled *Administering Certificate Services* and *Certificate Services Web Pages*. A brief description is provided below.

You can request a certificate in one of two ways:

- Use Internet Explorer to connect to a Web enrollment page. An enrollment page is provided with Windows 2000 Certificate Services and is installed on the same computer as the Certificate Service. To use these to request a certificate, connect to http://*servername*/CertSrv, and follow the directions. If you are using an enterprise CA, these pages require authentication, and you must select a template type to request a valid template. Typically, this will be a user template. You can also use Internet Explorer to request a certificate form a third-party commercial CA. Trusted root certificates are included in Windows 2000 for a number of these commercial CAs.
- Use the Certificate Manager snap-in to request a certificate from Microsoft Certificate Service. These procedures are described next.

To use Certificate Manager to request a certificate

1. Open the Microsoft Management Console (MMC).
2. Click **Console**, and then click **Add/Remove Snap-in**.
3. Click **Add**.
4. Click **Certificate Manager**, and click **Add**.
5. Select **My user account**, and click **Close**.
6. Click **Close** to close the Add/Remove snap-in.
7. Expand **Certificates** and **User** to open the certificate folder.
8. Select from the **View\Options** menu.
9. Check the **Logical Certificate Stores**, and click **OK**.
10. Expand **Personal** to open the folder. If you already have a certificate, you will have a **certificates** subfolder; otherwise, the folder will be empty.
11. Right-click **Personal**.
12. Select **All Tasks**.
13. Select **Request New Certificate**.
14. Follow the instructions to get a user certificate.

Exporting the Certificate

Once you have the certificate, you need to export it for use in later steps.

To export your certificate

1. Open MMC.
2. Click **Console**, and then click **Add/Remove Snap-in**.
3. Click **Add**.
4. Click **Certificates**, and click **Add**.
5. Select **My user account**, and click **Finish**.
6. Click **Close** to close the Add/Remove snap-in.
7. Double-click **Certificates** and **User** to open the certificate folder.
8. Select from the menu **View\Options** menu.
9. Check the **Logical Certificate Stores**, and click **OK**.
10. Double-click **Personal**. If there is no certificates subfolder, you do not have a certificate and must request one. See the previous procedure.
11. Open the **Certificates** subfolder.
12. Right-click a certificate issued to your account. Do not select a file recovery certificate.
13. Select **AllTask**, and then click **Export**.
14. Click **Next**.
15. Verify that **Do not export the private key** is selected, and click **Next**.
16. Select **Base 64 encode x.509**, and click **Next**.
17. Type a file name, and click **Next**.
18. Click **Finish**.

INSTALLING CA CERTIFICATES

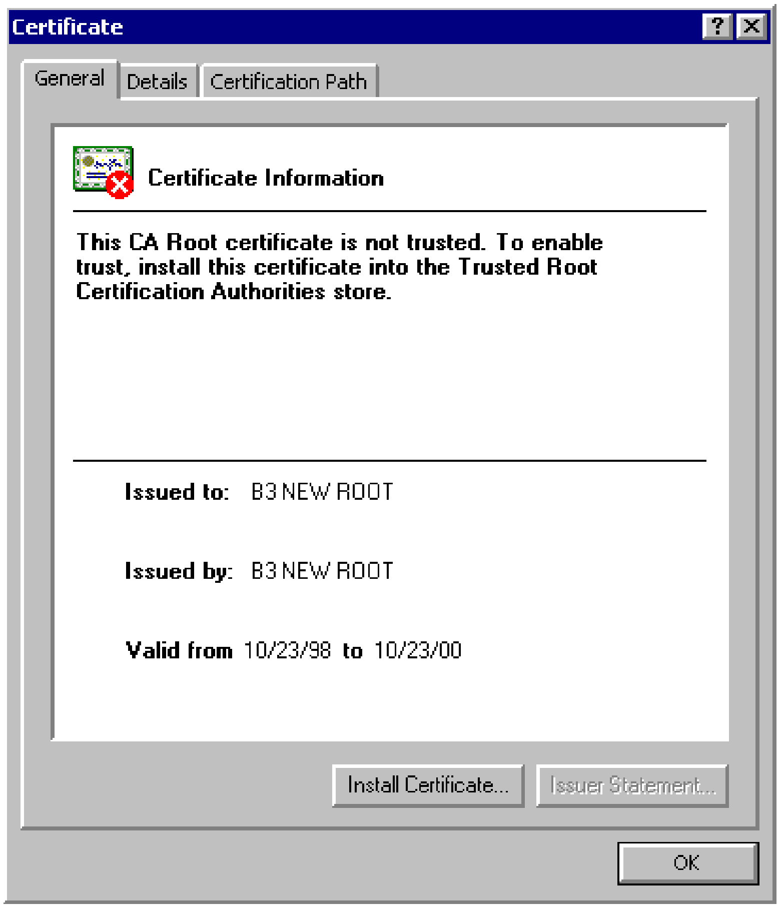
If you are using an enterprise CA in your domain, skip this section because the root certificate is trusted by your system.

If you are using some other CA, install the root CA and all intermediate roots into the machine store of the Web server. This is necessary so that the web server can verify the client certificate that you requested above.

Retrieve the CA certificate. If the CA is a Windows 2000 Certificate Service, you can retrieve the CA's certificate from the CA Web pages. See the walkthrough entitled *Certificate Services Web Pages*.

To install the CA certificates

1. Make sure you are logged on as an administrator.
2. Open the CA certificate by double-clicking the certificate file.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate into the Trusted Root Certification Authorities store.

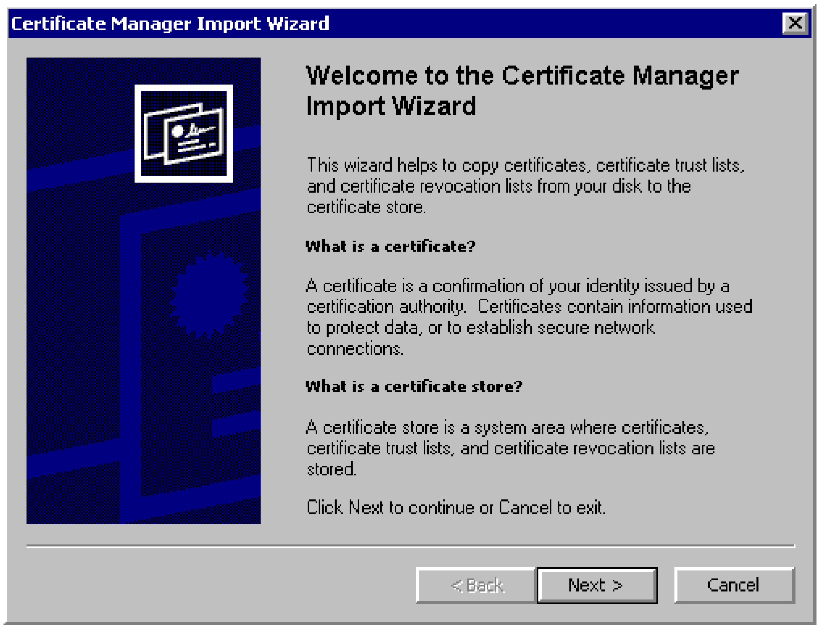
Issued to: B3 NEW ROOT

Issued by: B3 NEW ROOT

Valid from 10/23/98 to 10/23/00

Figure 1. Certificate information

3. Click the **Install Certificate** button.



Welcome to the Certificate Manager Import Wizard

This wizard helps to copy certificates, certificate trust lists, and certificate revocation lists from your disk to the certificate store.

What is a certificate?

A certificate is a confirmation of your identity issued by a certification authority. Certificates contain information used to protect data, or to establish secure network connections.

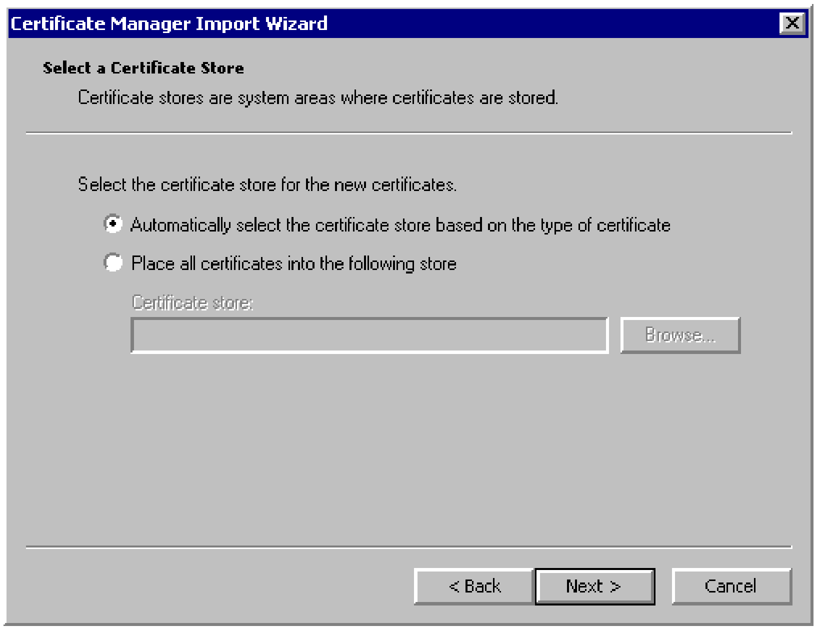
What is a certificate store?

A certificate store is a system area where certificates, certificate trust lists, and certificate revocation lists are stored.

Click Next to continue or Cancel to exit.

Figure 2. Certificate Manager Import Wizard

4. Click **Next**.



Select a Certificate Store

Certificate stores are system areas where certificates are stored.

Select the certificate store for the new certificates.

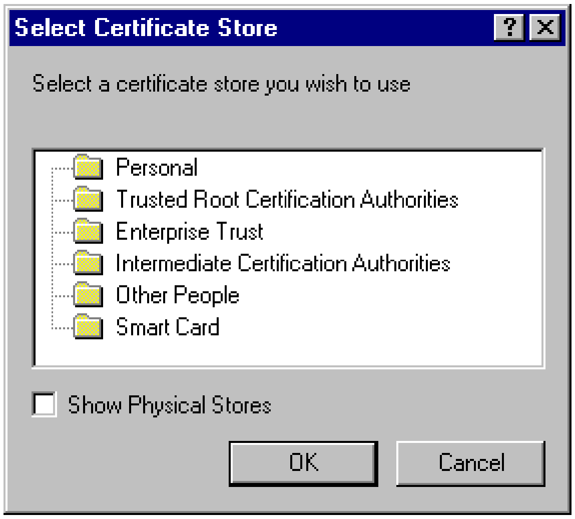
● Automatically select the certificate store based on the type of certificate

○ Place all certificates into the following store

Certificate store:

Figure 3. Selecting a certificate store

5. Select **Place all certificates into the following store**; then select **Browse**. If you use the automatic option, the CA certificates are placed in the user store, rather than the machine store. If this happens, you can use the Certificate Manager snap-in and drag the roots from one store to the other.



Select Certificate Store

Select a certificate store you wish to use

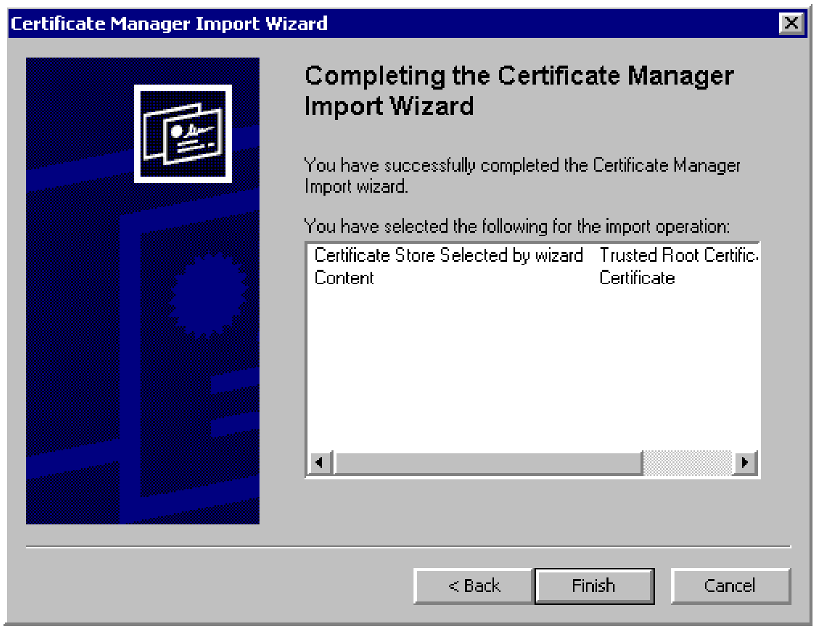
Figure 4. Certificate Manager snap-in

6. Check **Show Physical Stores**.

7. Expand the **Trusted Root Certification Authorities** or the **Intermediate Certification Authorities** depending on what type of CA certificate you are installing.

8. Select **Local Computer**, and click **OK**.

9. Click **Next**.



Completing the Certificate Manager Import Wizard

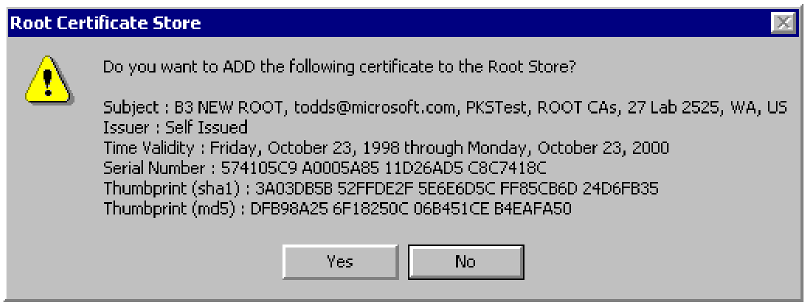
You have successfully completed the Certificate Manager Import wizard.

You have selected the following for the import operation:

Certificate Store Selected by wizard	Trusted Root Certific.
Content	Certificate

Figure 5. Completing the Certificate Manager Import Wizard

10. Click **Finish**.

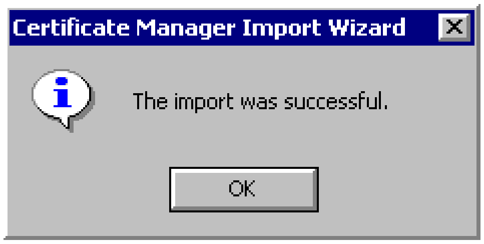


Do you want to ADD the following certificate to the Root Store?

Subject : B3 NEW ROOT, todds@microsoft.com, PKSTest, ROOT CAs, 27 Lab 2525, WA, US
Issuer : Self Issued
Time Validity : Friday, October 23, 1998 through Monday, October 23, 2000
Serial Number : 574105C9 A0005A85 11D26AD5 C8C7418C
Thumbprint (sha1) : 3A03DB5B 52FFDE2F 5E6E6D5C FF85CB6D 24D6FB35
Thumbprint (md5) : DFB98A25 6F18250C 06B451CE B4EAFA50

Figure 6. Warning that you are adding a root

11. A warning will appear that you are adding a root. Click **Yes**.



The import was successful.

Figure 7. Successful completion

12. Click **OK**.

Repeat these steps for each CA certificate.

If you have only one CA, you will have only a root certificate. Some user certificates that you receive from third-party CAs will be in a hierarchy in which there is a root CA and multiple intermediates above the user certificate.

PREPARING IIS FOR MAPPING

In this section, you configure IIS to do mapping.

Active Directory Mapping

Skip this section if you do not want to use Active Directory mapping.

To configure Active Directory mapping

1. Open the IIS snap-in, and right-click the server name in which IIS is running. Select **Properties**.

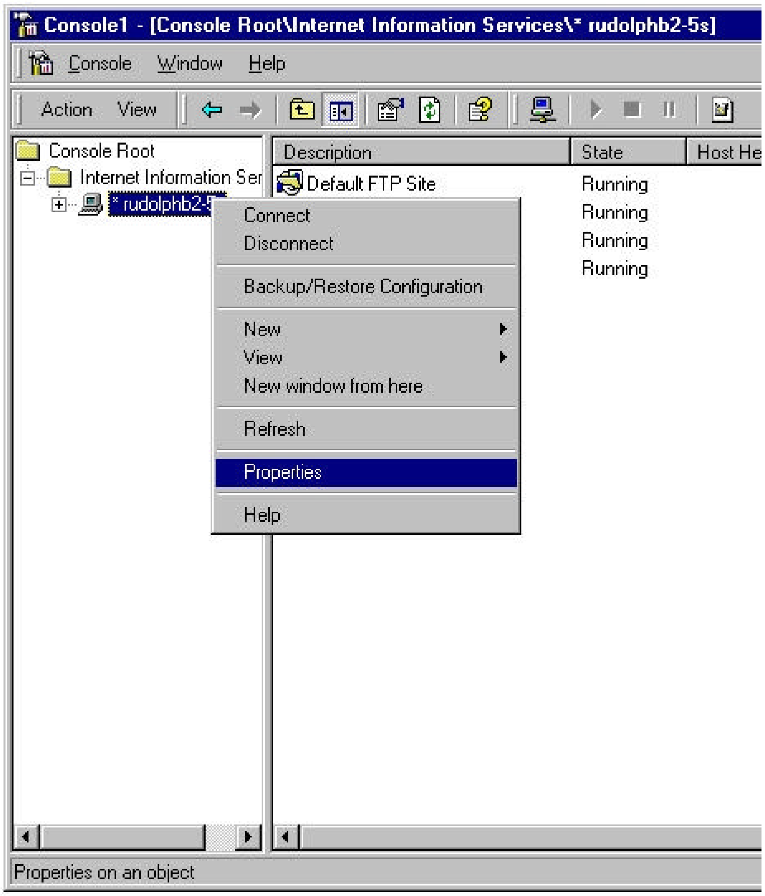
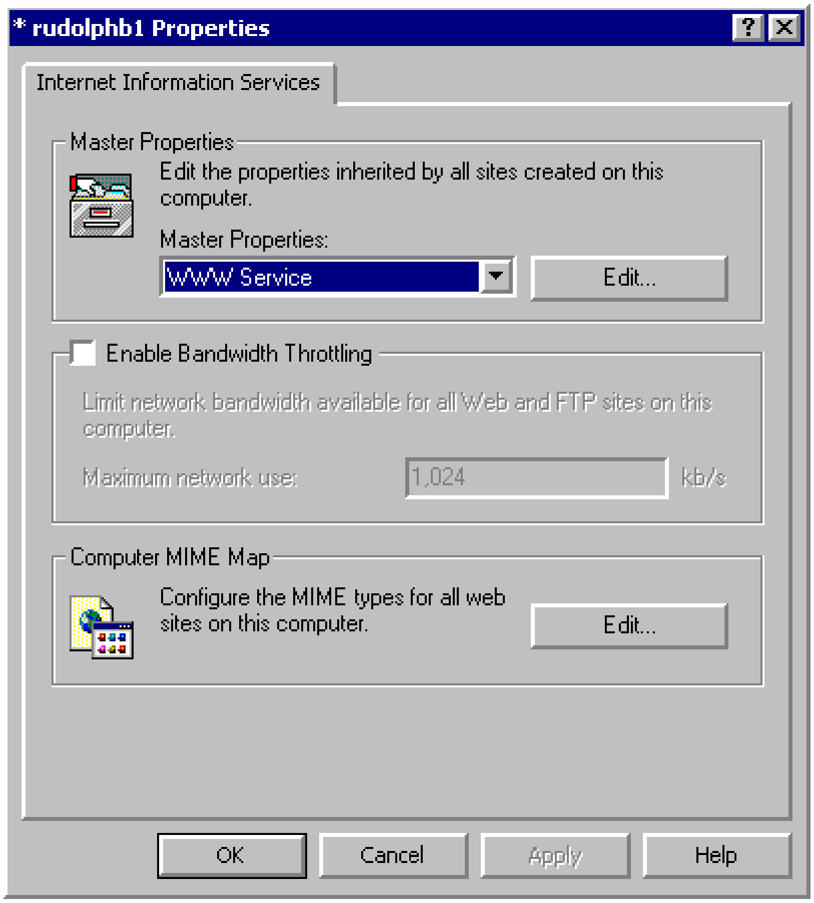


Figure 8. Viewing server properties

2. Click the **Edit** button in the **Master Properties** section.



rudolphb1 Properties

Internet Information Services

Master Properties

Edit the properties inherited by all sites created on this computer.

Master Properties: WWW Service

Edit...

□ Enable Bandwidth Throttling

Limit network bandwidth available for all Web and FTP sites on this computer.

Maximum network use: 1,024 kb/s

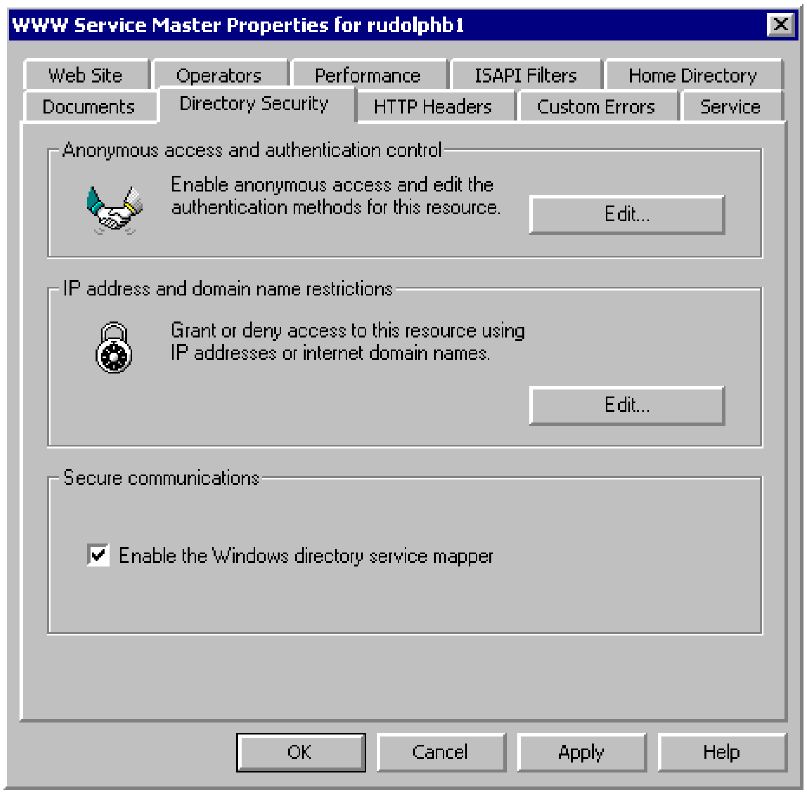
Computer MIME Map

Configure the MIME types for all web sites on this computer.

Edit...

Figure 9. Editing properties

3. Check the **Enable the Windows directory service mapper** checkbox. This option tells IIS that when you set a Web site to do mapping, it should really do Active Directory mapping. If this setting is unchecked, IIS does the mapping. Click **OK**.



WWW Service Master Properties for rudolphb1

Anonymous access and authentication control

Enable anonymous access and edit the authentication methods for this resource.

IP address and domain name restrictions

Grant or deny access to this resource using IP addresses or internet domain names.

Secure communications

☑ Enable the Windows directory service mapper

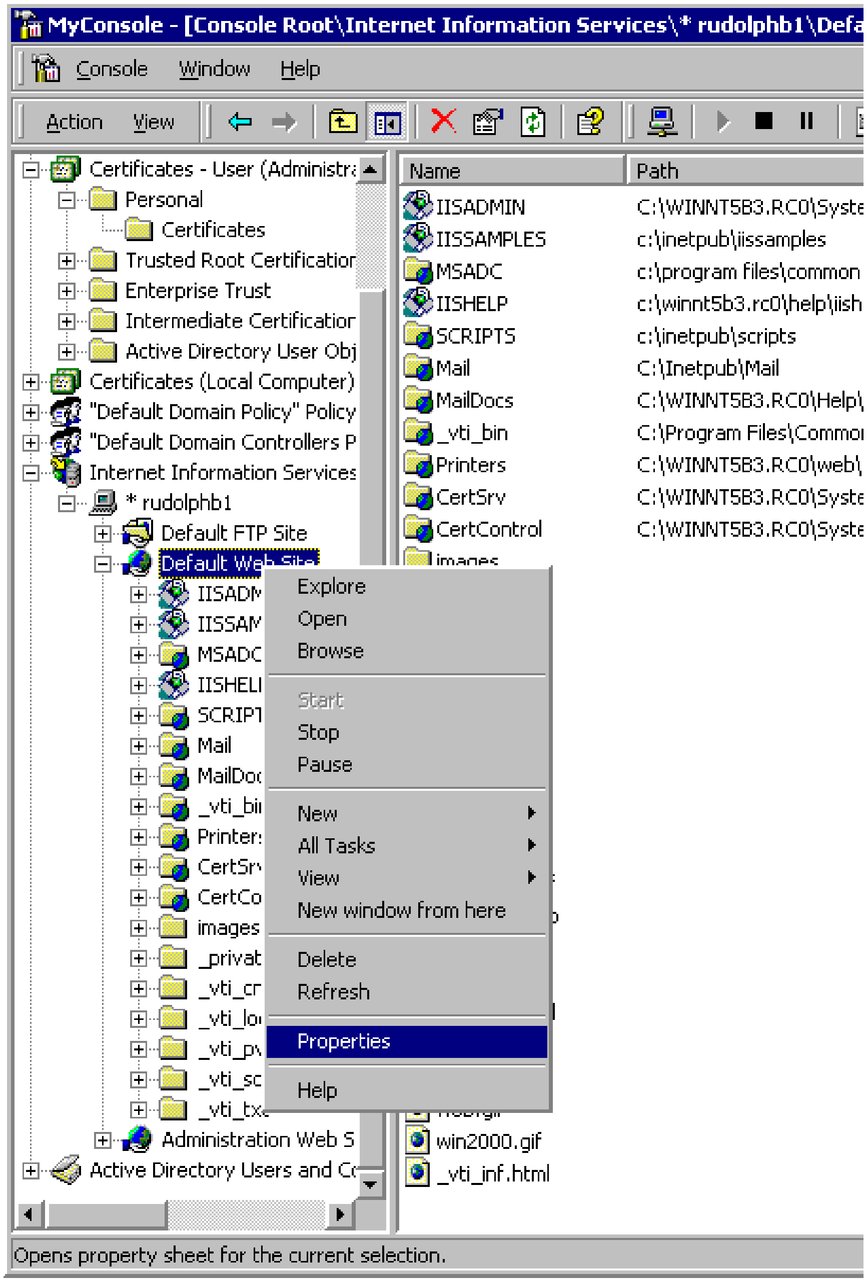
Figure 10. Enabling the directory to do mapping

Configuring SSL

The next step is to configure a site to use SSL. You must do this for both Active Directory and IIS mapping.

To configure the site to use SSL

1. In the IIS MMC snap-in, right-click the **Default Web Site** and select **Properties**.

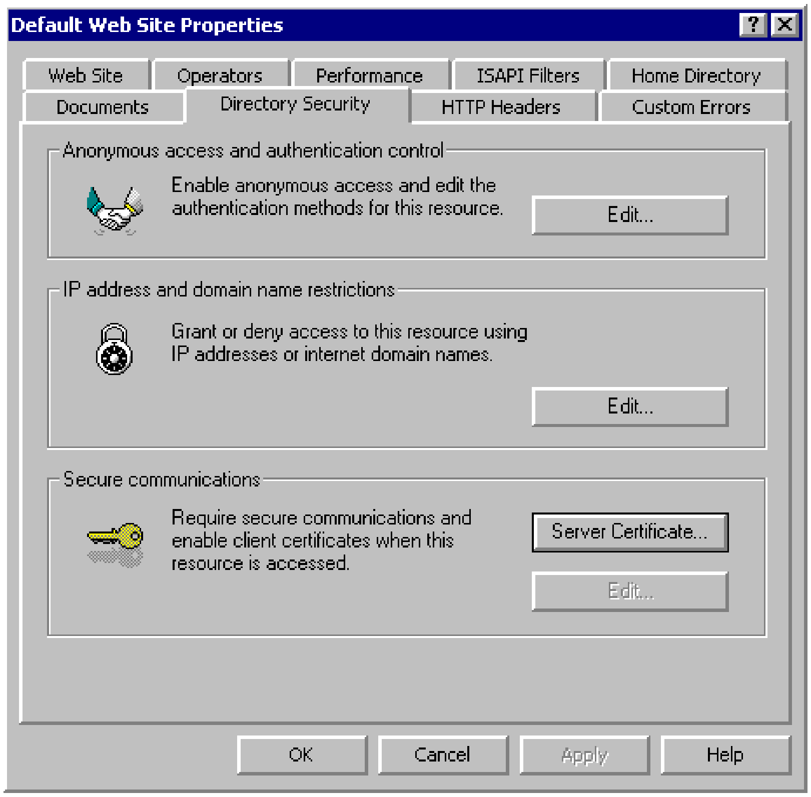


Name	Path
IISADMIN	C:\WINNT5B3.RC0\Syste
IISSAMPLES	c:\inetpub\iissamples
MSADC	c:\program files\common
IISHELP	c:\winnt5b3.rc0\help\iish
SCRIPTS	c:\inetpub\scripts
Mail	C:\Inetpub\Mail
MailDocs	C:\WINNT5B3.RC0\Help\
_vti_bin	C:\Program Files\Commo
Printers	C:\WINNT5B3.RC0\web\
CertSrv	C:\WINNT5B3.RC0\Syste
CertControl	C:\WINNT5B3.RC0\Syste
images	
win2000.gif	
_vti_inf.html	

Opens property sheet for the current selection.

Figure 11. Selecting Web site properties

2. Click the **Directory Security** tab.



Enable anonymous access and edit the authentication methods for this resource.

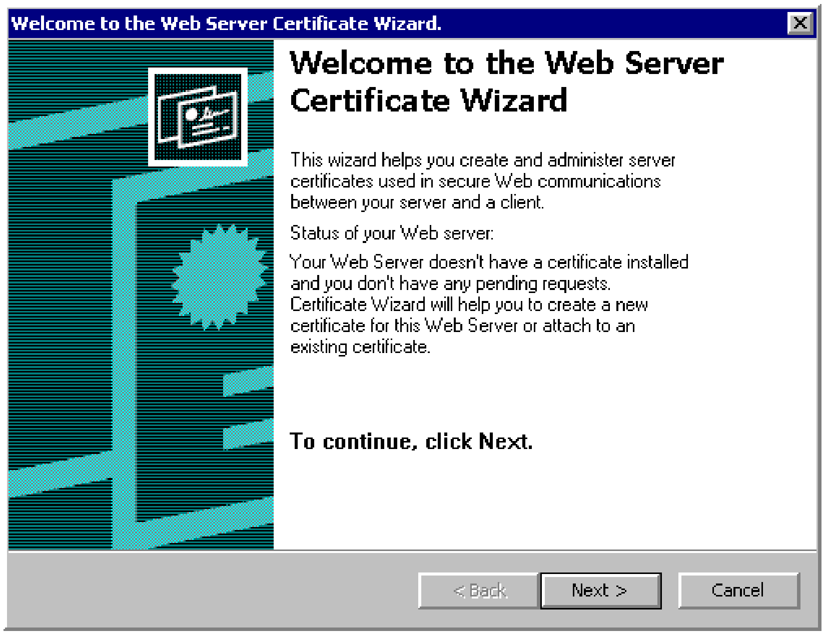
Grant or deny access to this resource using IP addresses or internet domain names.

Require secure communications and enable client certificates when this resource is accessed.

Figure 12. Default Web site properties page

Notice that the **Edit** button under Secure communications is unavailable. This is the case until you request a Web server certificate.

3. Click the **Server Certificate** button.



Welcome to the Web Server Certificate Wizard.

Welcome to the Web Server Certificate Wizard

This wizard helps you create and administer server certificates used in secure Web communications between your server and a client.

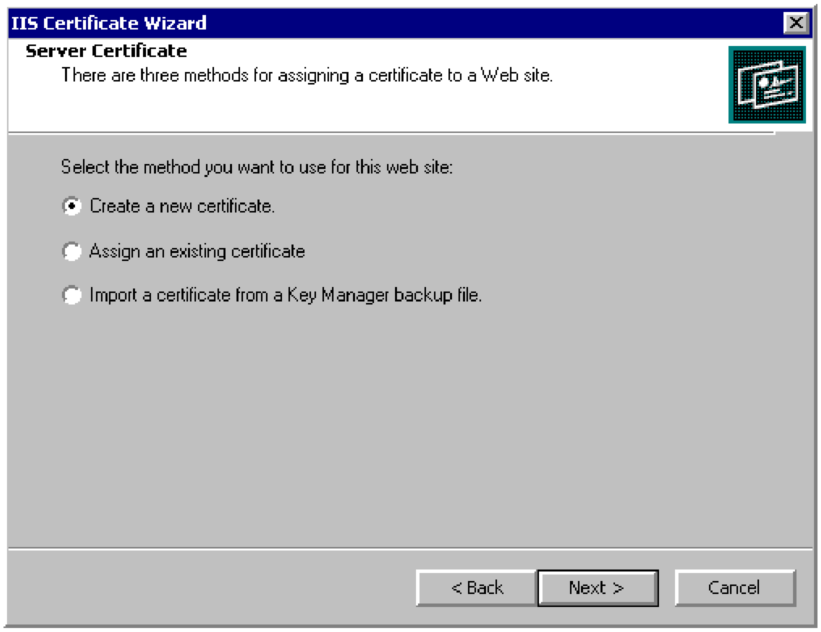
Status of your Web server:

Your Web Server doesn't have a certificate installed and you don't have any pending requests. Certificate Wizard will help you to create a new certificate for this Web Server or attach to an existing certificate.

To continue, click Next.

Figure 13. Web Server Certificate Wizard

4. Click **Next**.



IIS Certificate Wizard

Server Certificate

There are three methods for assigning a certificate to a Web site.

Select the method you want to use for this web site:

● Create a new certificate.

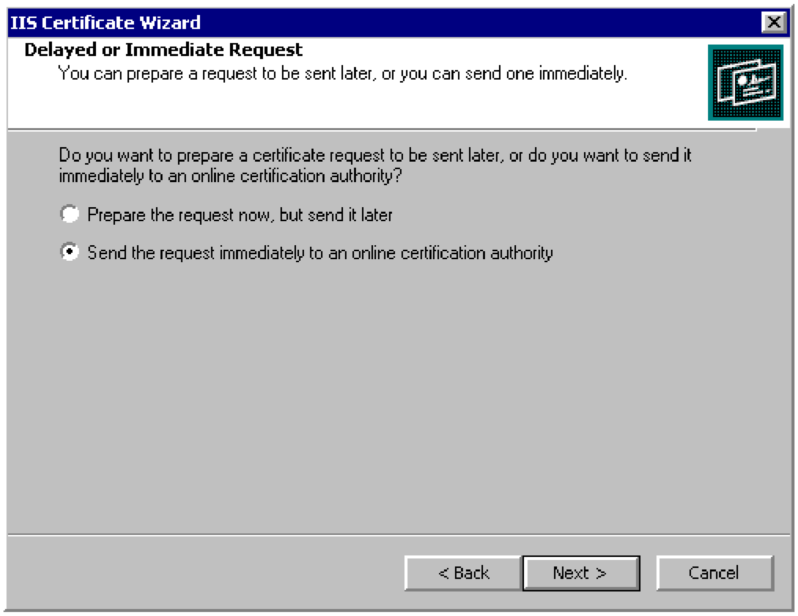
○ Assign an existing certificate

○ Import a certificate from a Key Manager backup file.

Figure 14. Selecting the method for assigning a certificate

5. Select **Create a New certificate**, and click **Next**. You will see a different dialog box if IIS already has a certificate.

6. Select **Send the request immediately to an online certification authority**. (This assumes that you have an enterprise CA in your domain that is configure to issue Web certificates. See the Casetup.doc walkthrough for details on setting up the an enterprise CA.)



IIS Certificate Wizard

Delayed or Immediate Request

You can prepare a request to be sent later, or you can send one immediately.

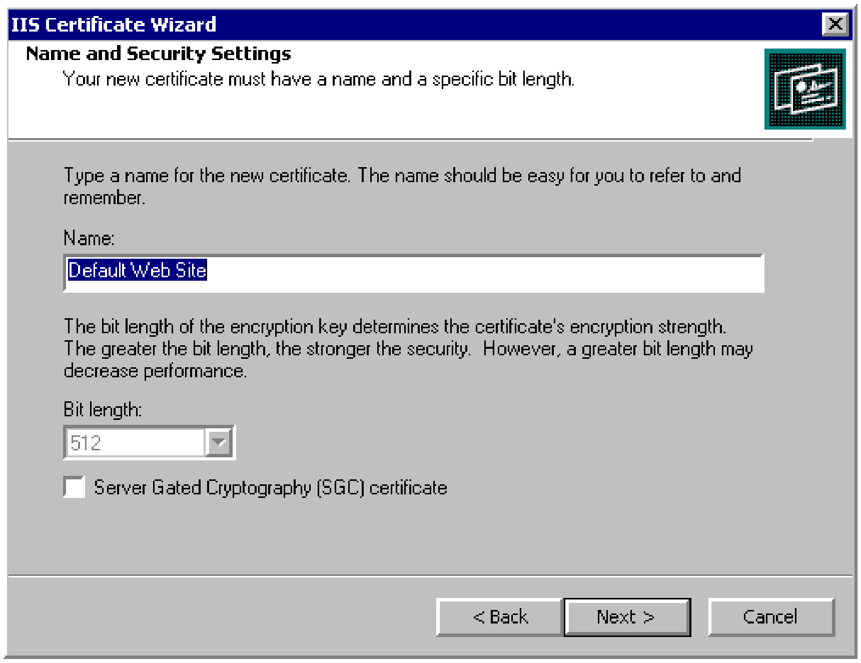
Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?

○ Prepare the request now, but send it later

● Send the request immediately to an online certification authority

Figure 15. Requesting immediate certificate delivery

7. Click **Next**.



IIS Certificate Wizard

Name and Security Settings

Your new certificate must have a name and a specific bit length.

Type a name for the new certificate. The name should be easy for you to refer to and remember.

Name: Default Web Site

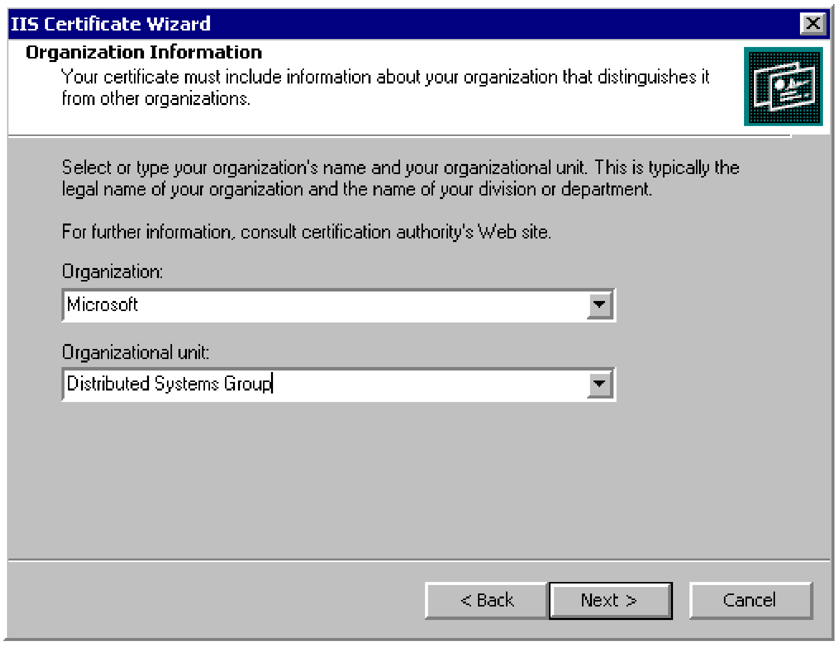
The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Bit length: 512

□ Server Gated Cryptography (SGC) certificate

Figure 16. Name and security settings

8. Click **Next**. You should not change any of these options.



IIS Certificate Wizard

Organization Information

Your certificate must include information about your organization that distinguishes it from other organizations.

Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

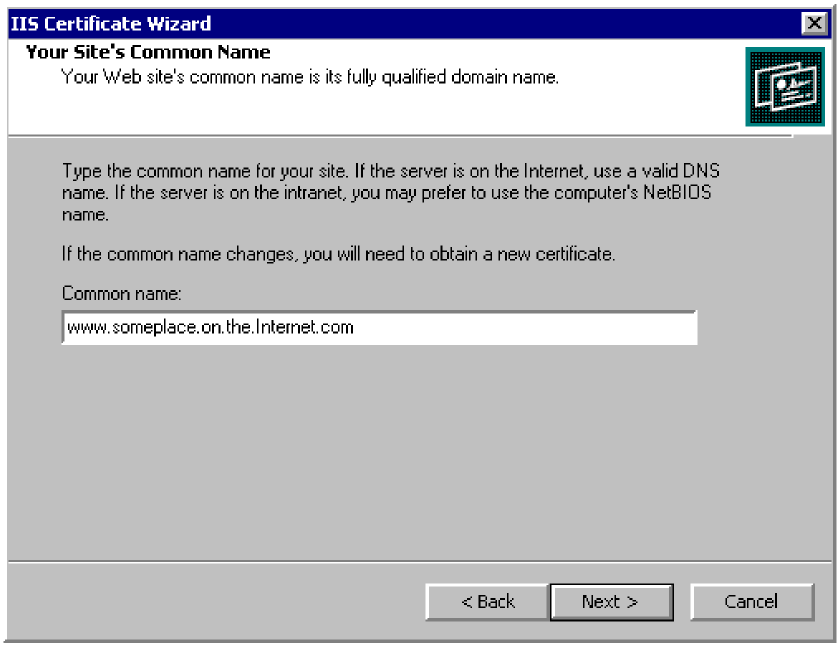
For further information, consult certification authority's Web site.

Organization: Microsoft

Organizational unit: Distributed Systems Group

Figure 17. Entering organization information

9. Enter your information, and click **Next**.



Your Site's Common Name

Your Web site's common name is its fully qualified domain name.

Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

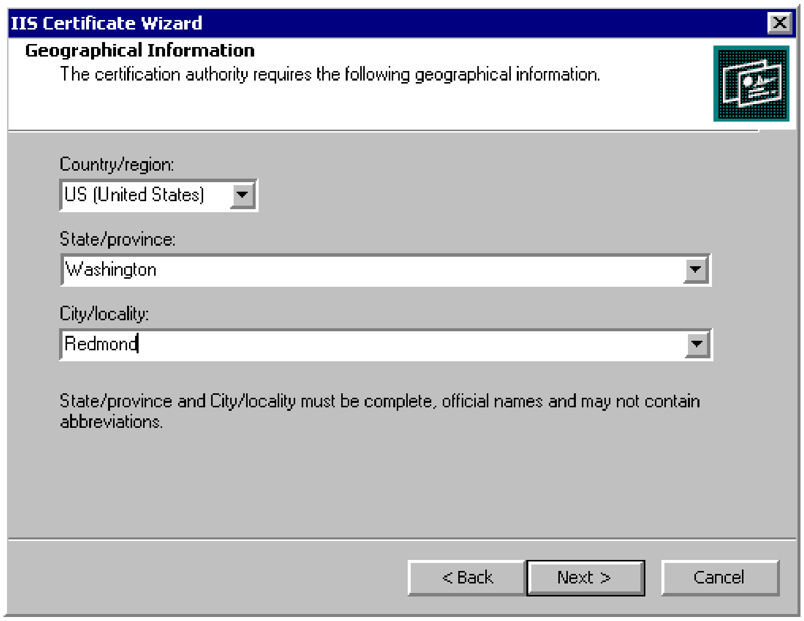
If the common name changes, you will need to obtain a new certificate.

Common name:

www.someplace.on.the.Internet.com

Figure 18. Entering your server name

10. Type your server name in the browser. It can be either the DNS name, the NetBIOS name, or the word LOCALHOST. Enter your choice, and click **Next**.



Geographical Information

The certification authority requires the following geographical information.

Country/region: US (United States)

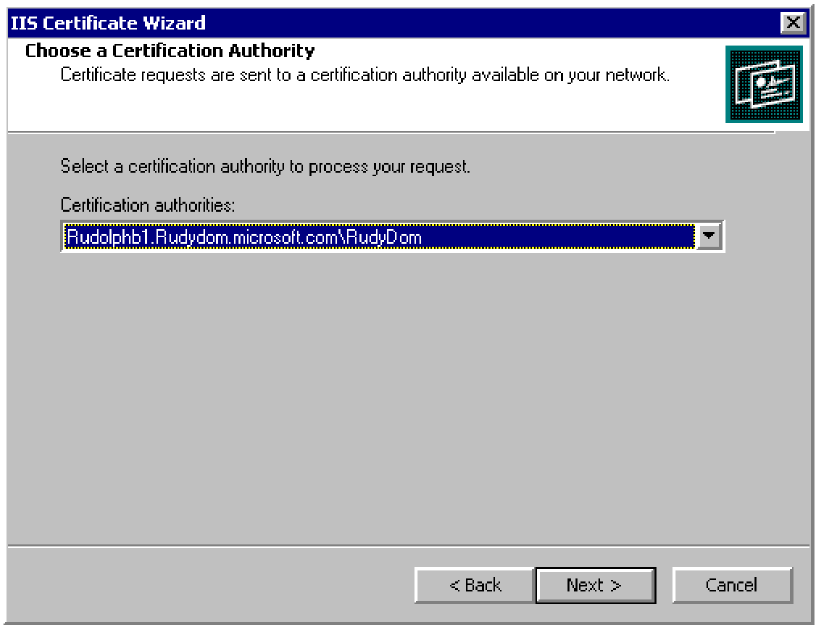
State/province: Washington

City/locality: Redmond

State/province and City/locality must be complete, official names and may not contain abbreviations.

Figure 19. Entering geographical information

11. Enter your information, and click **Next**.



IIS Certificate Wizard

Choose a Certification Authority

Certificate requests are sent to a certification authority available on your network.

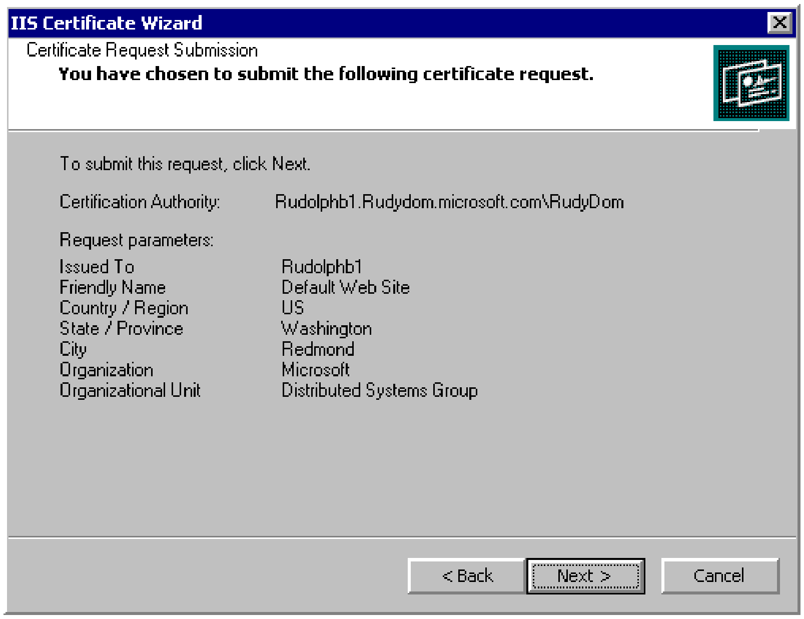
Select a certification authority to process your request.

Certification authorities:

Rudolphb1.Rudydom.microsoft.com\RudyDom

Figure 20. Choosing a certificate authority

12. If you have an enterprise CA in your domain from which you are allowed to request Web server certificates, you will see them listed here. If there is no CA, it is not configured to issue Web server certificates, or you do not have permission to request a Web server certificate, this list will be empty. Make your selection, and click **Next**.



Certificate Request Submission

You have chosen to submit the following certificate request.

To submit this request, click Next.

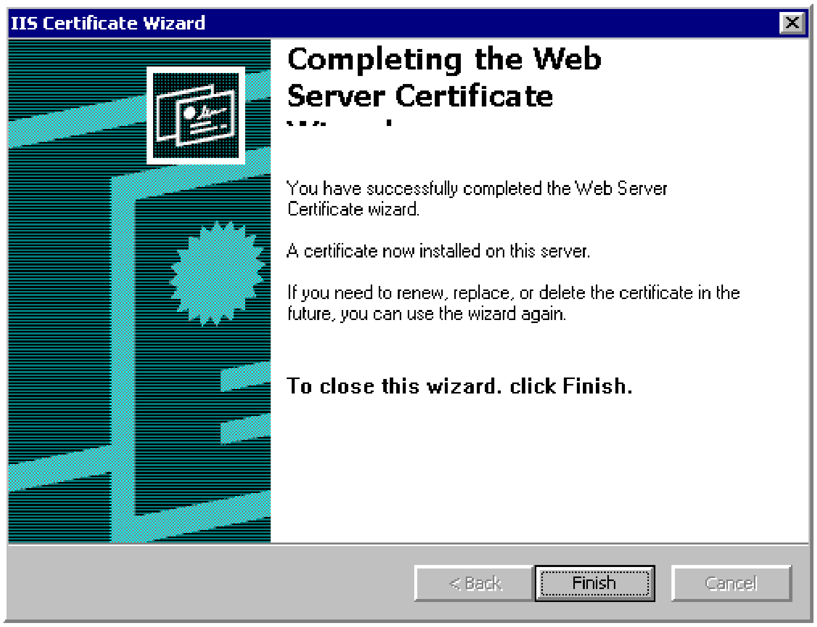
Certification Authority: Rudolphb1.Rudydom.microsoft.com\RudyDom

Request parameters:

Issued To	Rudolphb1
Friendly Name	Default Web Site
Country / Region	US
State / Province	Washington
City	Redmond
Organization	Microsoft
Organizational Unit	Distributed Systems Group

Figure 21. Verifying your choices

13. Click **Next**.



Completing the Web Server Certificate Wizard

You have successfully completed the Web Server Certificate wizard.

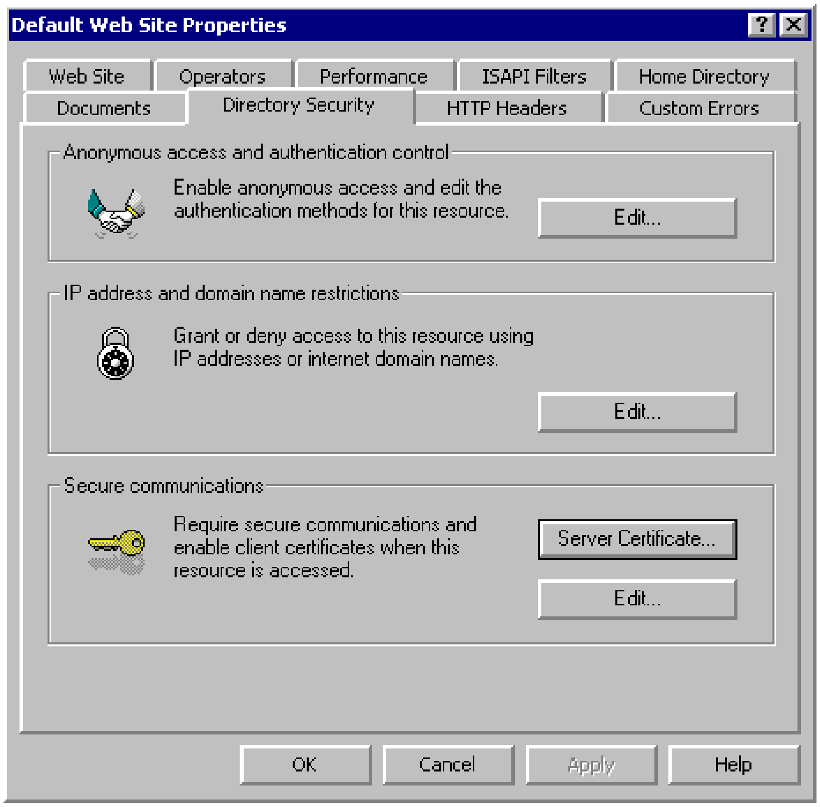
A certificate now installed on this server.

If you need to renew, replace, or delete the certificate in the future, you can use the wizard again.

To close this wizard, click Finish.

Figure 22. Successful completion

14. Click **Finish**. The server now has a server certificate.



Anonymous access and authentication control

Enable anonymous access and edit the authentication methods for this resource.

IP address and domain name restrictions

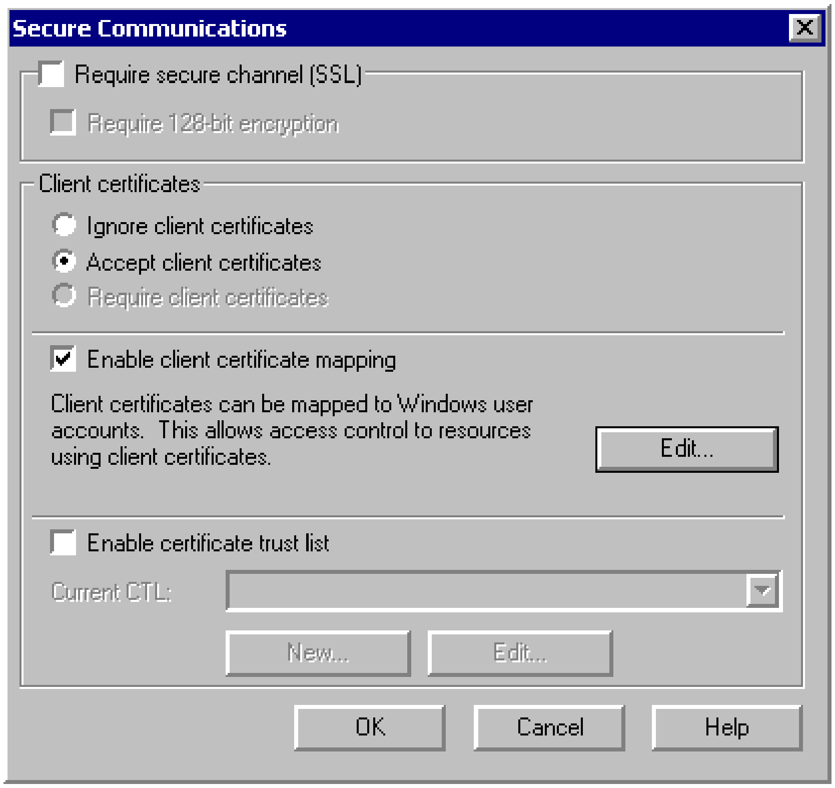
Grant or deny access to this resource using IP addresses or internet domain names.

Secure communications

Require secure communications and enable client certificates when this resource is accessed.

Figure 23. Secure communications with Edit button enabled

15. You will notice the **Edit** button under **Secure communication** is now enabled. Click the **Edit** button.



Secure Communications

□ Require secure channel (SSL)

□ Require 128-bit encryption

Client certificates

○ Ignore client certificates

● Accept client certificates

○ Require client certificates

☑ Enable client certificate mapping

Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

□ Enable certificate trust list

Current CTL:

Figure 24. Configuring the site for SSL and account mapping

16. You can now use this dialog box to configure the site to do SSL and account mapping. You must check the **Enable client certificate mapping** for both IIS and Active Directory mapping. Select either **Accept client certificates** or **Require client certificates**. The **Accept client certificates** setting requires negotiation of client certificate authentication with the browser. If it fails, it falls back to one of the standard authentication protocols. If you select **Require client certificates**, you must also check the **Require secure channel** checkbox. No fallback is allowed to another authentication method. Requiring secure channel means that the Web site will not be viewable through HTTP, only through HTTPS. You should not check the **Enable certificate trust list** for this walkthrough. See the section, "Known Issues," for a note on 128-bit encryption.

Mapping User Accounts

If you are doing Active Directory mapping, skip this section**.**

If you want to do IIS mapping, first be sure that you turn off Active Directory mapping. IIS is now ready to do certificate mapping.

ONE-TO-ONE MAPPING

This section covers one-to-one mapping, first in the Active Directory and then with IIS.

Using the Active Directory for One-to-One Mapping

If you have set IIS to do directory mapping by following the instructions above, IIS automatically does UPN mapping for certificates from a trusted enterprise CA. You can go to the section, "Testing the Mapping," below, to see UPN mapping. The default administrator account does not have a UPN and does not map. You must create a new account and use its certificate to see UPN mapping.

To configure Active Directory one-to-one mapping

1. Open the Active Directory Users and Computers snap-in.

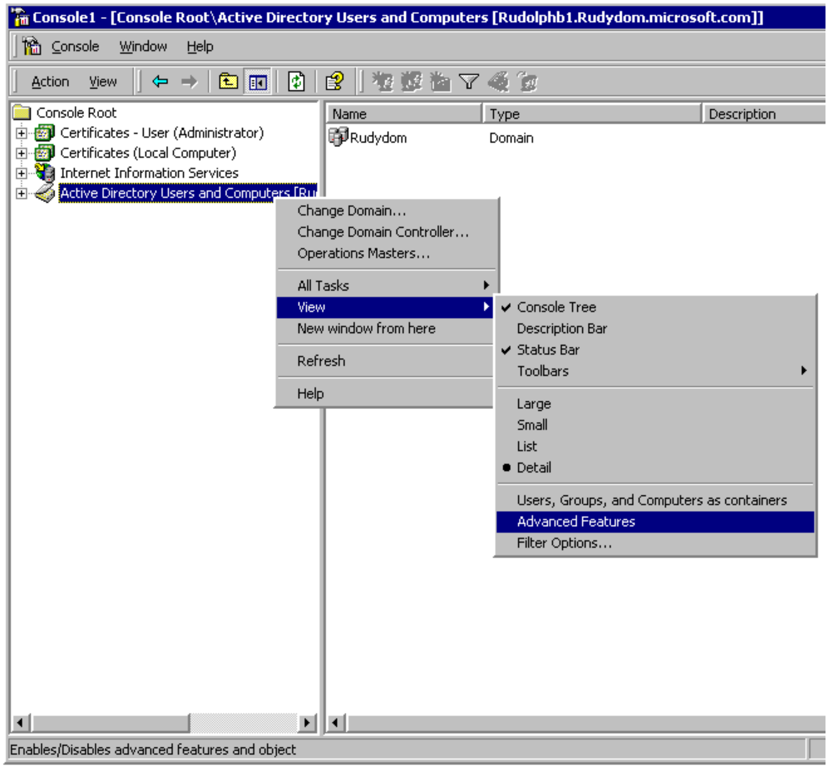

Console1 - [Console Root\Active Directory Users and Computers [Rudolphb1.Rudydom.microsoft.com]]
Console
Window
Help
Action
View
Console Root
Certificates - User (Administrator)
Certificates (Local Computer)
Internet Information Services
Active Directory Users and Computers [Ru
Name
Type
Description
Rudydom
Domain
Change Domain...
Change Domain Controller...
Operations Masters...
All Tasks
View
New window from here
Refresh
Help
✓ Console Tree
Description Bar
✓ Status Bar
Toolbars
Large
Small
List
● Detail
Users, Groups, and Computers as containers
Advanced Features
Filter Options...
Enables/Disables advanced features and object

Figure 25. Active Directory Users and Computers snap-in

2. Right-click the snap-in, select **View**, and then select **Advanced Features**.

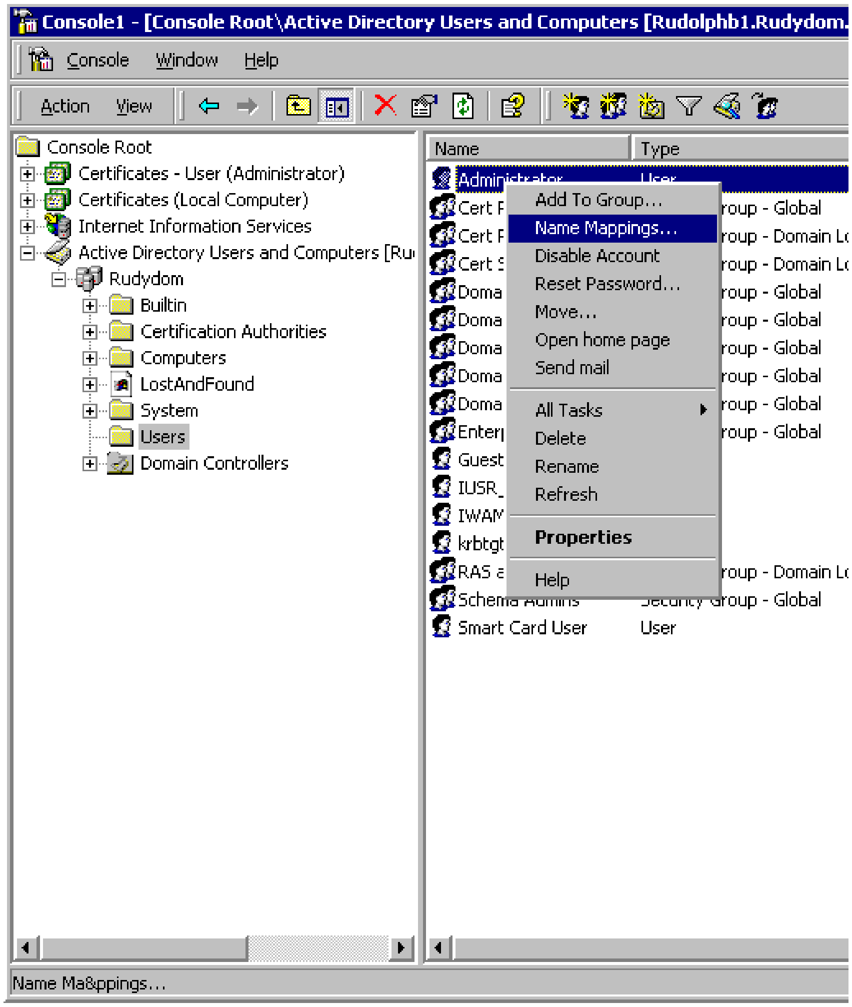
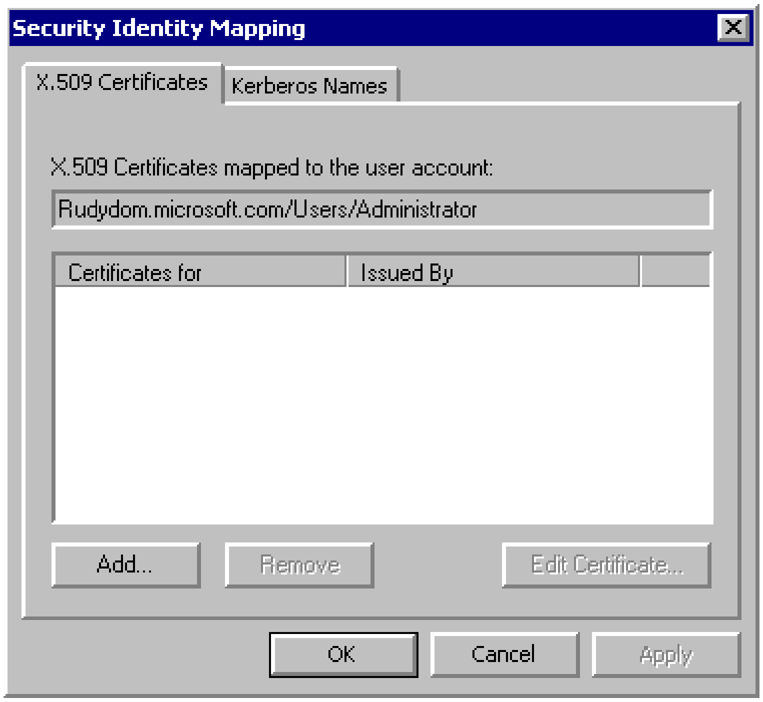


Figure 26. Selecting name mappings

3. Right-click the **Administrator** account. Select **Name Mappings**.

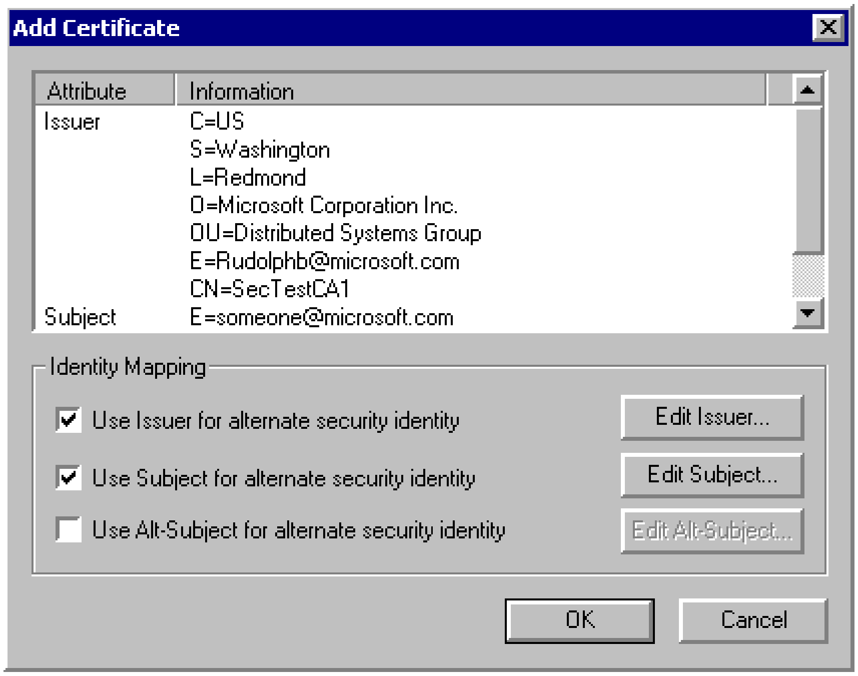


X.509 Certificates mapped to the user account:

Rudydom.microsoft.com/Users/Administrator

Figure 27. Adding a user certificate

4. Click the **Add** button. Select the user certificate from the .cer file saved in the **Exporting a certificate** section.



Attribute	Information

Issuer	C=US
	S=Washington
	L=Redmond
	O=Microsoft Corporation Inc.
	OU=Distributed Systems Group
	E=Rudolphb@microsoft.com
	CN=SecTestCA1

Subject	E=someone@microsoft.com

☑ Use Issuer for alternate security identity

☑ Use Subject for alternate security identity

☐ Use Alt-Subject for alternate security identity

Figure 28. The Add Certificate dialog box

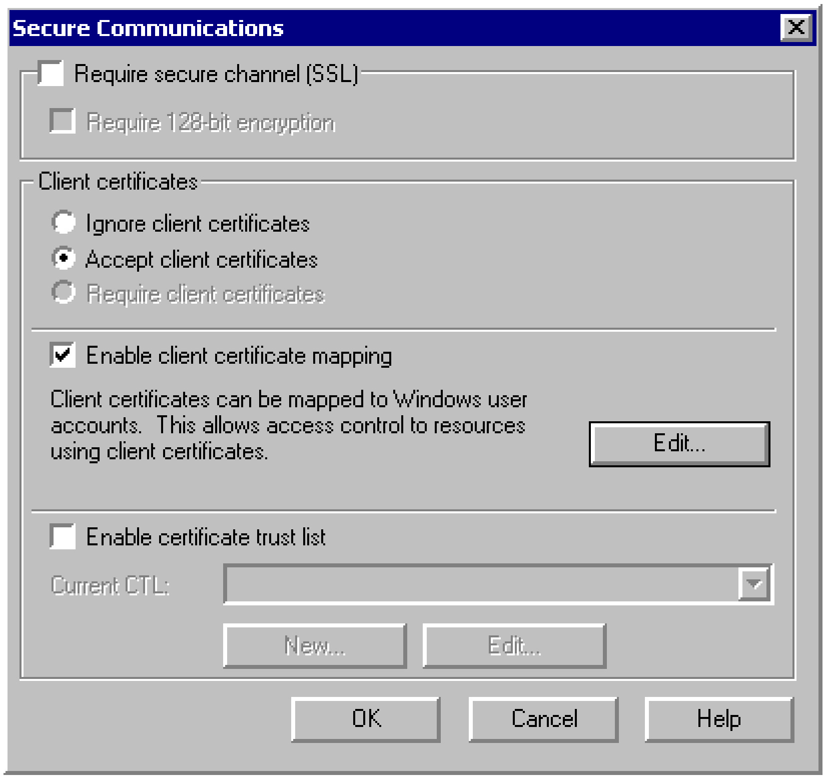
5. If you leave both **Use Issuer for alternate security identity** and **Use Subject for alternate security identity** checked, you will be doing one-to-one mapping. By unchecking either, you will be doing many-to-one mapping. Click **OK**.

6. Go to the section, “Testing the Mapping,” later in this paper to verify that this works.

Using IIS for One-to-One Mapping

Instead of using the Active Directory as in the previous section, you can use IIS to do all the mappings. To configure IIS one-to-one mapping, first be sure that Active Directory mapping is turned off.

This is done by returning to the master property page and unchecking **Active Directory mapping**.



Secure Communications

□ Require secure channel (SSL)

□ Require 128-bit encryption

Client certificates

○ Ignore client certificates

● Accept client certificates

○ Require client certificates

☑ Enable client certificate mapping

Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

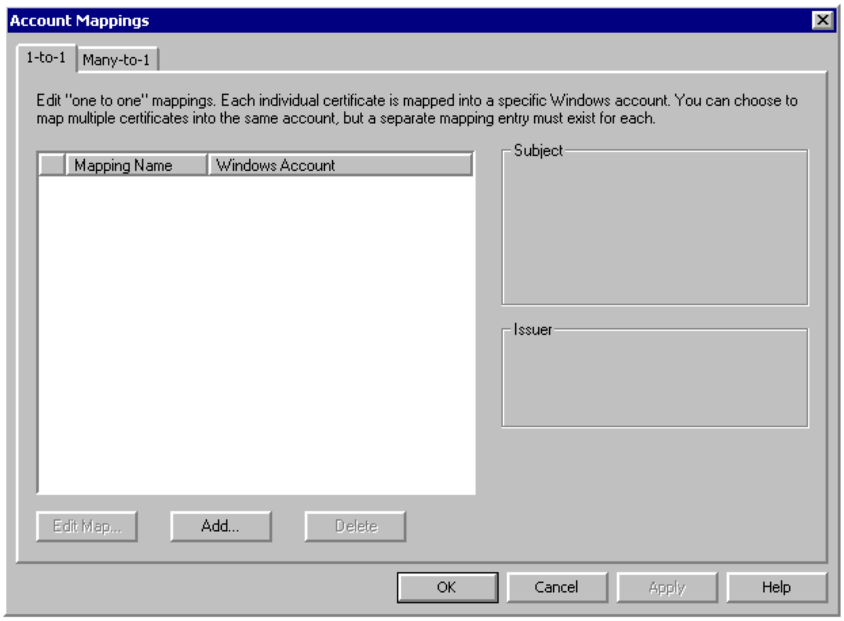
□ Enable certificate trust list

Current CTL:

Figure 29. Secure Communications dialog box

To configure IIS one-to-one mapping

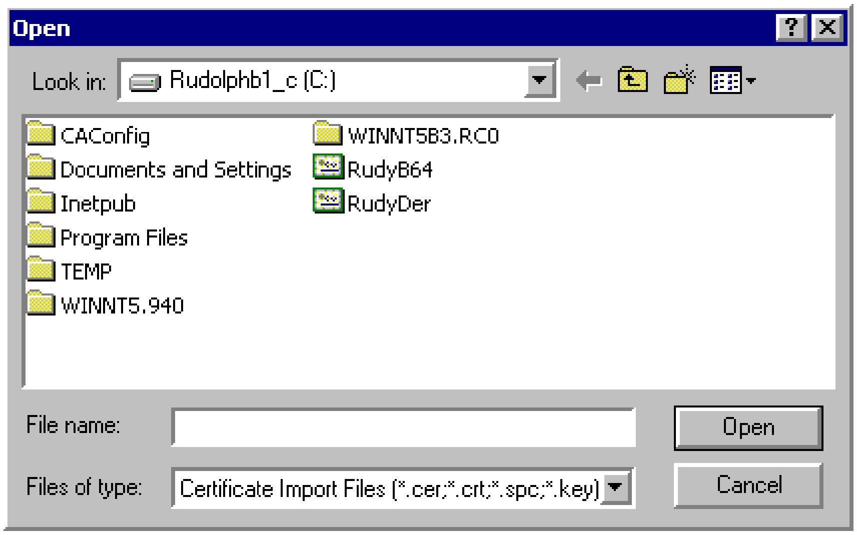
1. From the Secure Communications dialog box in the IIS snap-in, click the **Edit** button.



Edit "one to one" mappings. Each individual certificate is mapped into a specific Windows account. You can choose to map multiple certificates into the same account, but a separate mapping entry must exist for each.

Figure 30. Adding a one-to-one mapping

2. On the 1-to-1 tab, click **Add**.



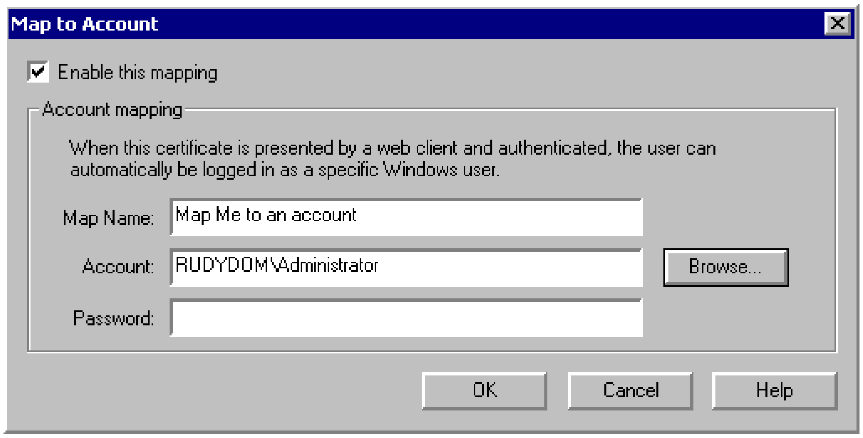
Look in: Rudolphb1_c (C:)

File name:

Files of type: Certificate Import Files (*.cer;*.crt;*.spc;*.key)

Figure 31. Selecting the user's certificate

3. Select the user's certificate. For IIS, this certificate must be base-64 encoded and cannot be a binary certificate. The dialog box above shows two certificates: Rudyb64 and RudyDer. IIS can only process Rudyb64, even though Windows 2000 works with both.


Map to Account

☑ Enable this mapping

Account mapping

When this certificate is presented by a web client and authenticated, the user can automatically be logged in as a specific Windows user.

Map Name: Map Me to an account

Account: RUDYDOM\Administrator

Password:

Figure 32. Completing the mapping

4. Click the **Browse** button to select the Administrator account. Click **OK** after entering the password.
5. Click **OK** to exit the IIS snap-in and apply the mapping.

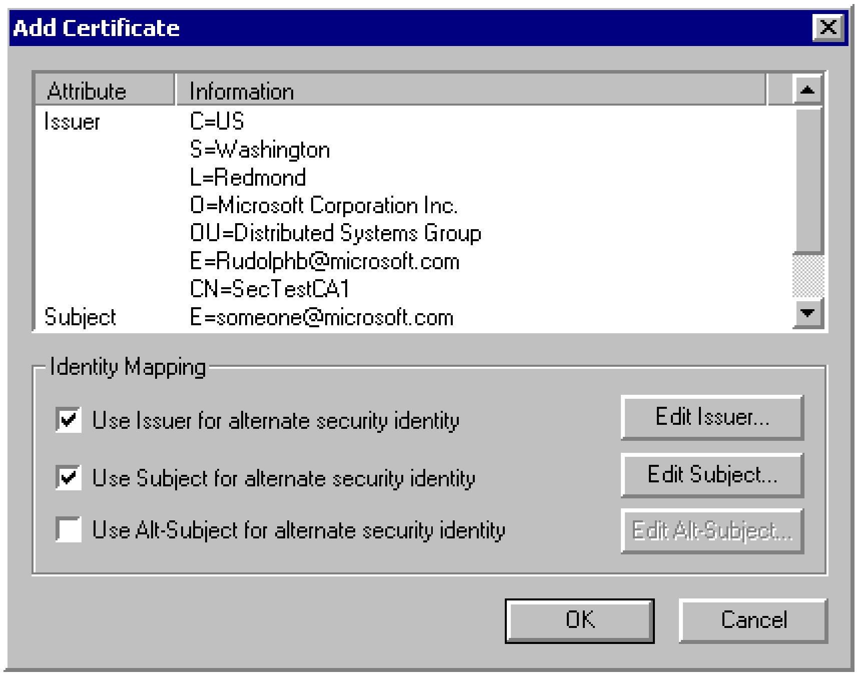
IIS one-to-one mapping is now configured. You can go to the section "Testing the Mapping" section at the end of this paper to see this mapping work.

MANY-TO-ONE MAPPING

In the previous two sections, you used one-to-one mapping. You will now configure many-to-one mapping in which many users (certificates) are mapped to a single Windows 2000 user account.

Using the Active Directory for Many-to-One Mapping

Repeat the steps you did for Active Directory in the one-to-one mapping section until you reach the dialog box below. Remember to enable Active Directory mapping if you disabled it in the previous section.



Attribute	Information
Issuer	C=US
	S=Washington
	L=Redmond
	O=Microsoft Corporation Inc.
	OU=Distributed Systems Group
	E=Rudolphb@microsoft.com
	CN=SecTestCA1
Subject	E=someone@microsoft.com

Identity Mapping

☑ Use Issuer for alternate security identity

☑ Use Subject for alternate security identity

☐ Use Alt-Subject for alternate security identity

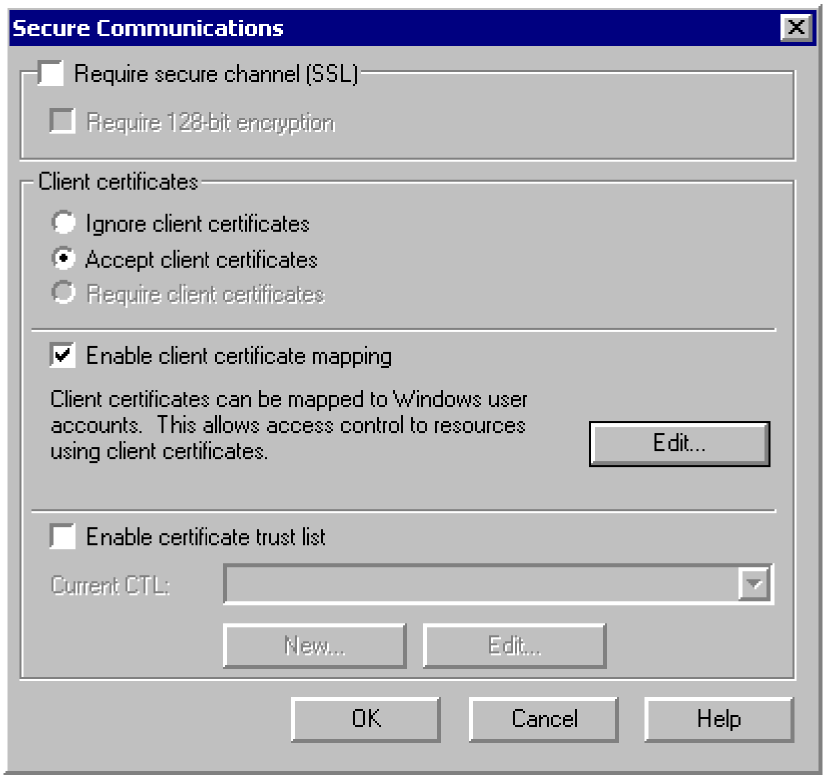
Figure 33. The Add Certificate dialog box

On this dialog box, uncheck **Use Subject for alternate security identity**, and click **OK**. You have now configured the Active Directory to map all certificates from the issuing CA to the Administrator account.

You can again go to the Testing the Mapping section and see that any certificate issued by this CA works to access the server.

Using IIS for Many-to-One Mapping

To configure IIS many-to-one mapping, be sure that directory mapping is turned off.



Secure Communications

☐ Require secure channel (SSL)

☐ Require 128-bit encryption

Client certificates

○ Ignore client certificates

● Accept client certificates

○ Require client certificates

☑ Enable client certificate mapping

Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

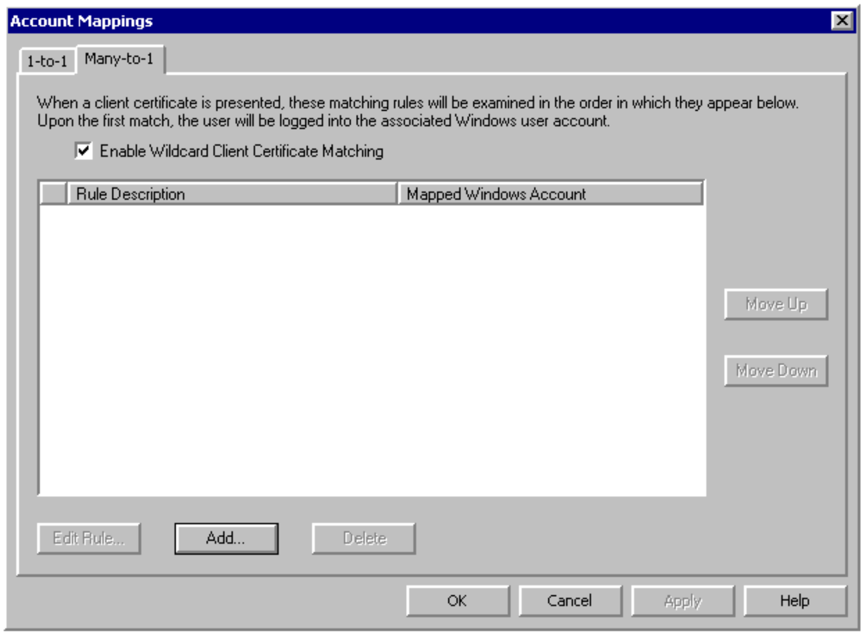
☐ Enable certificate trust list

Current CTL:

Figure 34, Secure Communications dialog box

To configure IIS many-to-one mapping

1. From the **Secure Communications** dialog box in the IIS snap-in, click the **Edit** button under **Enable client certificate mapping**.



Account Mappings

1-to-1 | Many-to-1

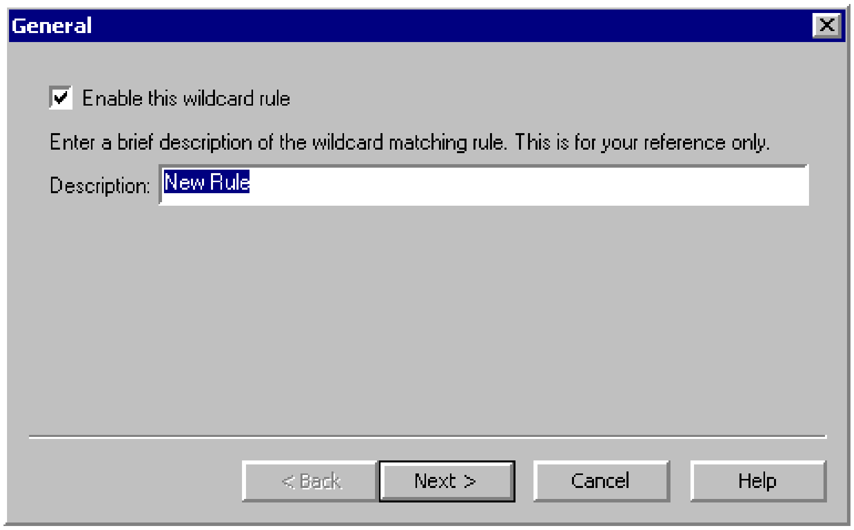
When a client certificate is presented, these matching rules will be examined in the order in which they appear below. Upon the first match, the user will be logged into the associated Windows user account.

☑ Enable Wildcard Client Certificate Matching

	Rule Description	Mapped Windows Account

Figure 35. The Many-to-1 tab

2. Click the **Many-to-1** tab. Click **Add**.



General

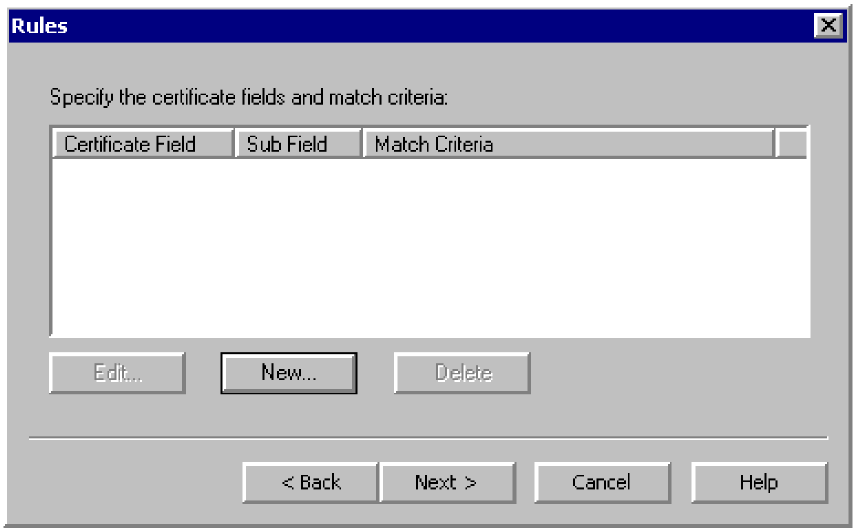
☑ Enable this wildcard rule

Enter a brief description of the wildcard matching rule. This is for your reference only.

Description: New Rule

Figure 36. Wildcard Rule dialog box

3. Click **Next**.

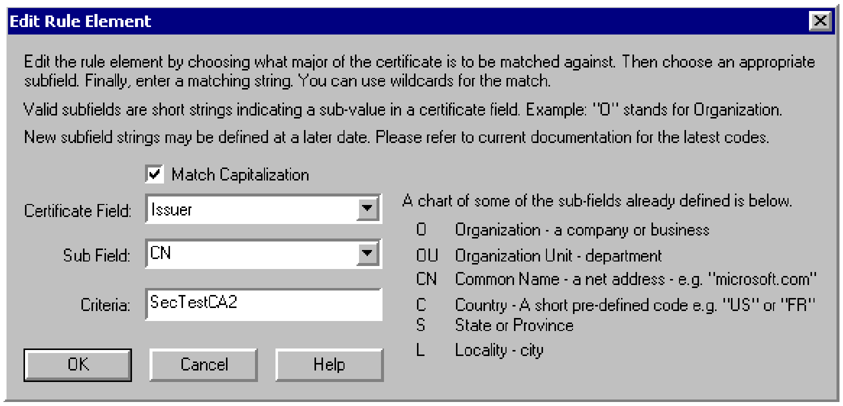


Specify the certificate fields and match criteria:

Certificate Field	Sub Field	Match Criteria

Figure 37. Creating new matching rules

4. Click **New**.



Edit the rule element by choosing what major of the certificate is to be matched against. Then choose an appropriate subfield. Finally, enter a matching string. You can use wildcards for the match.

Valid subfields are short strings indicating a sub-value in a certificate field. Example: "O" stands for Organization.

New subfield strings may be defined at a later date. Please refer to current documentation for the latest codes.

☑ Match Capitalization

Certificate Field: Issuer

Sub Field: CN

Criteria: SecTestCA2

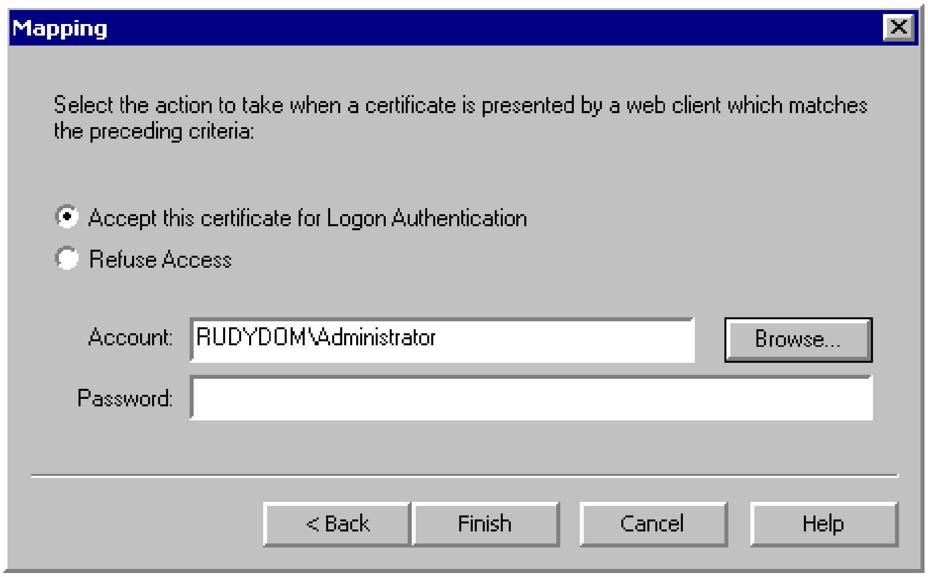
A chart of some of the sub-fields already defined is below.

O	Organization - a company or business
OU	Organization Unit - department
CN	Common Name - a net address - e.g. "microsoft.com"
C	Country - A short pre-defined code e.g. "US" or "FR"
S	State or Province
L	Locality - city

Figure 38. Entering your matching rules

5. You can enter as many fields as you wish to this rule. However, for this walkthrough, use only one. In the dialog box in Figure 38, specify that the CN in the Issuer name is equal to SecTestCA2. This means that all certificates issued by this CA will be mapped. Enter this information into your dialog box. Replace the **Criteria** with the value in your certificate. Click **OK**.

   See the section, “Known Issues,” below for a note on strings containing Unicode. All strings containing Unicode currently fail to map using IIS mapping. This includes all fields that contain the @ symbol. Select fields that contain only printable strings.



Mapping

Select the action to take when a certificate is presented by a web client which matches the preceding criteria:

● Accept this certificate for Logon Authentication

○ Refuse Access

Account: RUDYDOM\Administrator

Password:

Figure 39. Selecting the account

6. Click the **Browse** button to select the administrators account. Click **Finish**.

IIS is now configured to do many-to-one mapping. You can again go to the Testing the Mapping section to see this in action.

TESTING THE MAPPING

This section allows you to test the mappings that you have made.

Setting Up a Web Page

Typically, all the default Web pages that are installed with Windows 2000 are set so that any user can access the pages. To see certificate mapping in action, you must create a page that can be accessed only if mapping is occurring. The following two steps create a file and configure the access rights so that only a mapped user can access it. This file is used to verify that mapping is occurring.

Creating a Restricted File

First, create a file that can only be accessed by the Administrator account. This can by any type of file: .htm, .asp, .gif, .jpeg, and so on. For this test, use a .gif file.

To create a restricted file

1. Go to the **Inetpub\Wwwroot** directory with Windows Explorer.
2. Copy the file Windows2000.gif to Admin.gif.
3. Right-click on Admin.gif, and select **Properties**.
4. Click the **Security** tab.
5. Uncheck the **Allow inheritable permissions** at the bottom of the dialog box.
6. Remove all users and groups from this file.
7. Add **back** the Administrator account with **Full control**
8. Click **OK**.

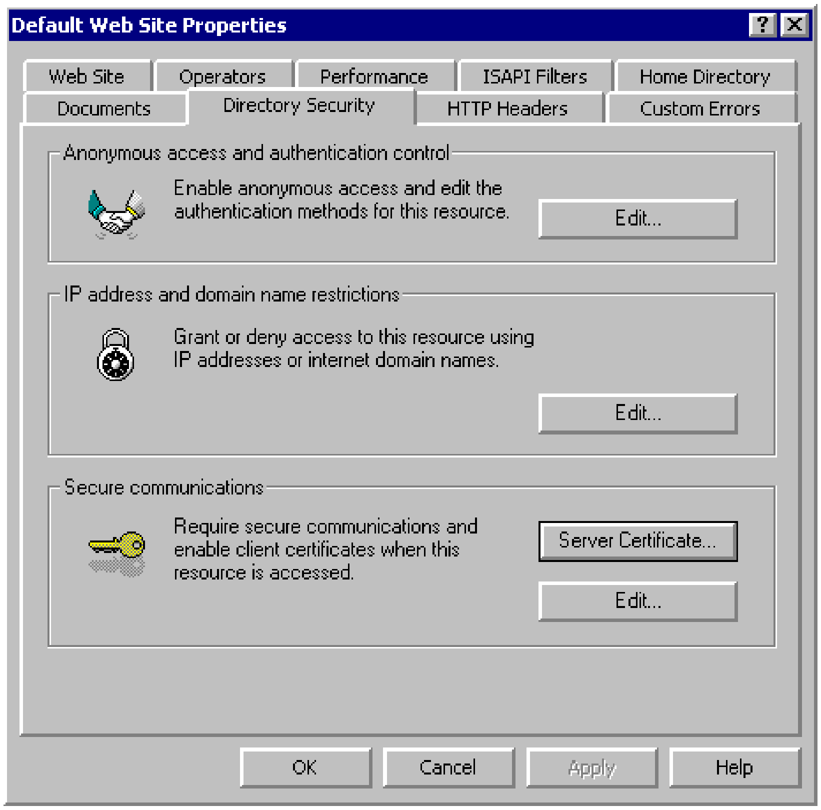
This file can now be accessed only by the Administrator account.

Turning Off Authentication

When IIS accesses a file, it impersonates a user so that the system uses the authenticated user's access rights. You need to ensure that the authentication happened using certificate mapping, rather than some other method.

To configure IIS so that no other form of authentication is possible for this file

1. Go to the IIS MMC snap-in.
2. Open **Default web site**.
3. In the right window, click on the file Admin.gif.
4. Select **Properties**.



Default Web Site Properties

Anonymous access and authentication control

Enable anonymous access and edit the authentication methods for this resource.

IP address and domain name restrictions

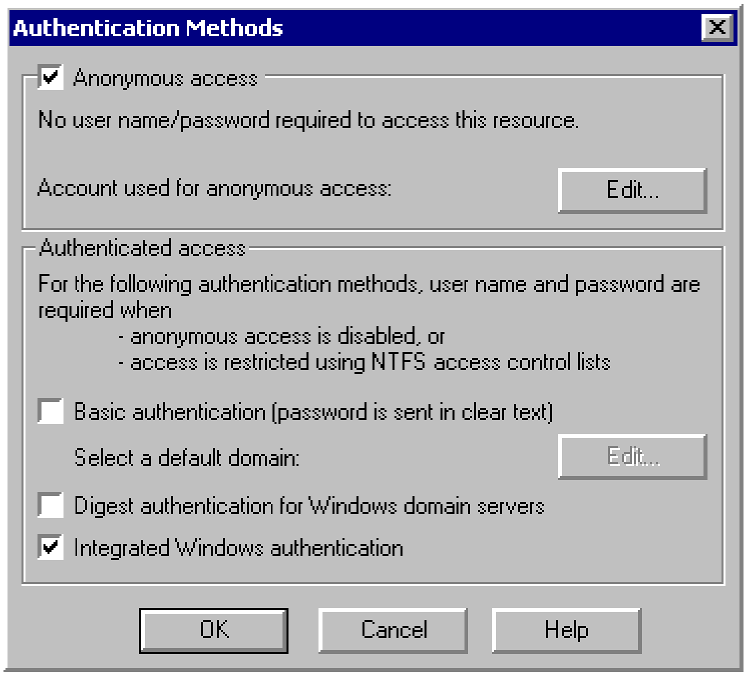
Grant or deny access to this resource using IP addresses or internet domain names.

Secure communications

Require secure communications and enable client certificates when this resource is accessed.

Figure 40. The Directory Security tab

5. Select the **Directory Security** tab
6. Click **Edit** under **Anonymous access and authentication control**.



Authentication Methods

☑ Anonymous access

No user name/password required to access this resource.

Account used for anonymous access:

Authenticated access

For the following authentication methods, user name and password are required when
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

□ Basic authentication (password is sent in clear text)

Select a default domain:

□ Digest authentication for Windows domain servers

☑ Integrated Windows authentication

Figure 41. Authentication Methods dialog box

7. Uncheck all options. (You can leave anonymous access if you want.)

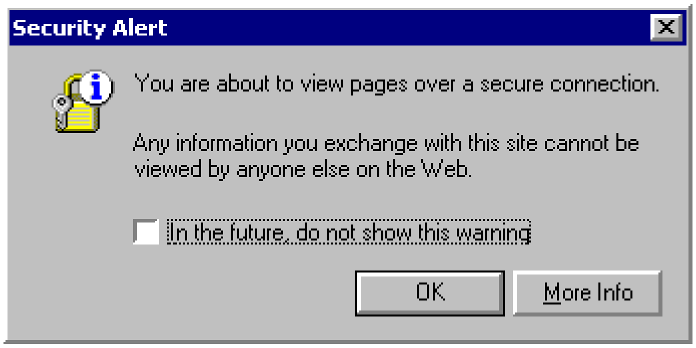
Go back to Internet Explorer, and try to access the page. If you succeed, the user has been authenticated using the mapping.

Connecting a Web Page

The next step is to connect to this file and verify that the mapping is working.

To connect to the file

1. From the **Start** menu, select **Run** and type https://*servername*/admin.gif where *servername* is the name of the Web server. If you are testing this on the Web server use LOCALHOST instead of the server name.



Security Alert

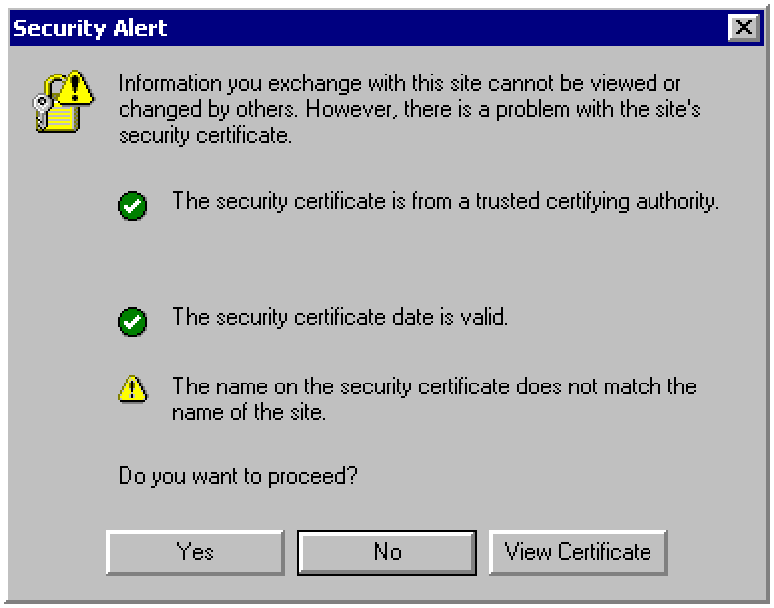
You are about to view pages over a secure connection.

Any information you exchange with this site cannot be viewed by anyone else on the Web.

□ In the future, do not show this warning

Figure 42. Security warning

2. Internet Explorer will probably display this warning that you are about to use SSL. Click **OK**.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

✓ The security certificate is from a trusted certifying authority.

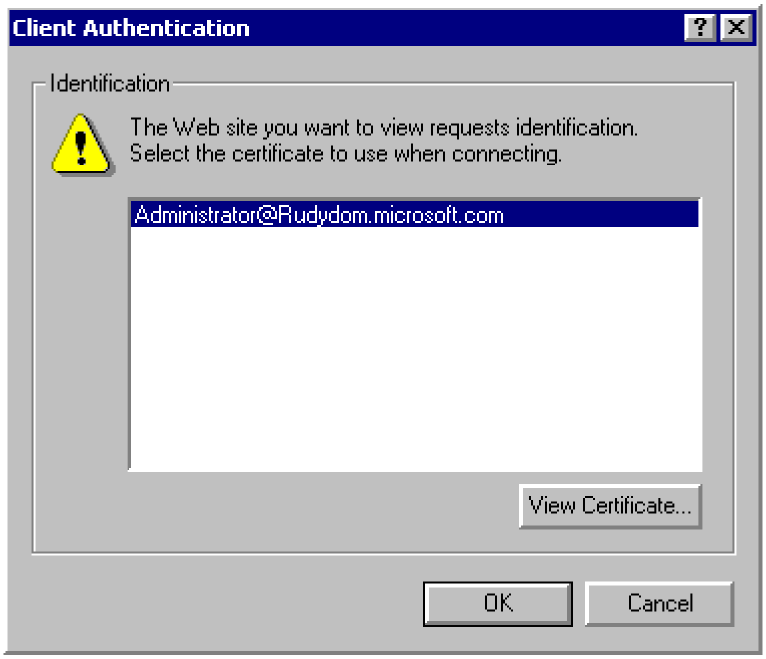
✓ The security certificate date is valid.

⚠ The name on the security certificate does not match the name of the site.

Do you want to proceed?

Figure 43. Nonmatching name warning

3. You will see this message if you used LOCALHOST to connect. Internet Explorer is warning you that the server certificate does not match the name that you typed. Click **Yes**.



Client Authentication

Identification

The Web site you want to view requests identification. Select the certificate to use when connecting.

Administrator@Rudydom.microsoft.com

Figure 44. Client identification

4. You should next see a selection of certificates. Select the certificate that you used in the mapping, and click **OK**. You should be doing this test from the computer on which you installed the certificate originally. Each certificate has a corresponding private key that is stored only on the computer on which you made the original user certificate request. For more information, see the Windows 2000 documentation.

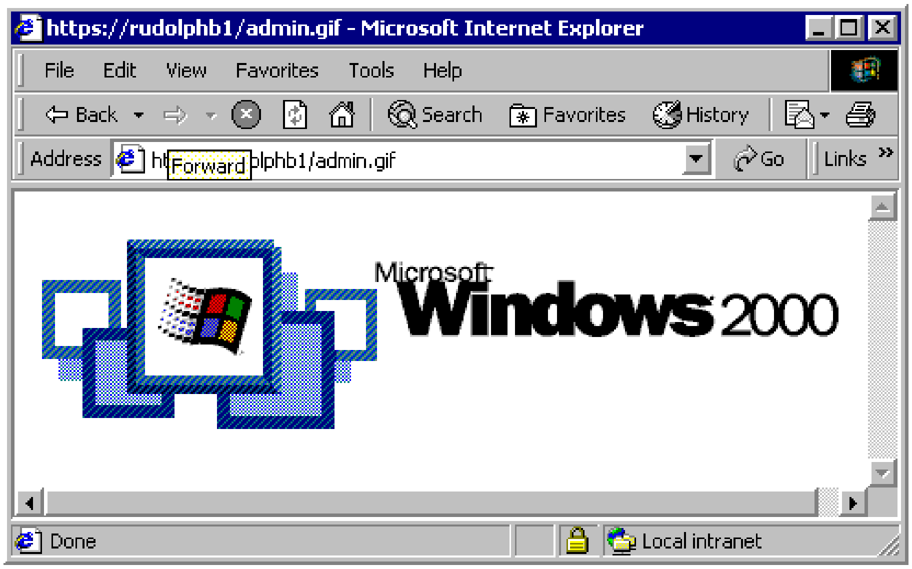


Figure 45. Opening the file

If the mapping worked you should see the .gif file.

If you see an error, there are a number of possible reasons:

- An access denied message indicates that you are successfully authenticating but that you do not have permissions to access the file. Check the permission on the file to see which account your certificate maps to.
- A certificate revoked message usually indicates that the certificate has been revoked or that IIS was unable to retrieve a certificate revocation list (CRL). You may need to install the CRL.
- A certificate is not trusted or is invalid message usually means that you have not installed the roots into the computer’s trusted root store on the Web server. A common mistake is to install the roots into the user’s trusted root store.

The error messages are usually quite descriptive. The release notes are another good place to look for information.

KNOWN ISSUES

The following sections cover known issues as of Beta 3.

Importing Certificates into IIS

IIS mapping code allows you to import only base-64 encoded certificate files. The file starts with Begin Certificate and ends with End Certificate.

Online Enrollment to Some CAs

Online enrollment can be done only to an enterprise CA. If the local CA is not an enterprise CA, you must create the certificate request to a file and process the request through the certificate server Web pages. Of course, if the CA is an external CA (such as VeriSign), you must do this anyway.

Requiring 128-bit Encryption

IIS does not generate a warning if you select 128-bit encryption even if the OS cannot provide that level of encryption.

Mapping Certificates with Unicode RDNs

If you are trying to do a many-to-one mapping in which one of the parts of the name you are mapping is encoded using Unicode, IIS mapping does not work. The typical case is an e-mail name, since the @ symbol forces the string to be stored as Unicode. Active Directory many-to-one mapping does not have this problem.

Misleading Revoked Certificate Error

IIS by default attempts to check the revocation status of a certificate. IIS indicates that a certificate is revoked even though the certificate is still valid if it cannot retrieve the CRL for that certificate. Ensure that the correct revocation list is installed in the machine store under **Enterprise/Certificate Revocation Lists**.

FOR MORE INFORMATION

For the latest information on Microsoft Windows 2000 network operating system, visit our World Wide Web site at http://www.microsoft.com/windows/server/ and the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

For the latest information on the Windows 2000 Beta 3, visit the Web site at http://ntbeta.microsoft.com

Before You Call for Support

Please keep in mind that Microsoft does not support these walkthroughs. The purpose of the walkthroughs is to facilitate your initial evaluation of the Microsoft Windows 2000 features. For this reason, Microsoft cannot respond to questions you might have regarding specific steps and instructions.

Reporting Problems

Problems with Microsoft Windows 2000 Beta 3 should be reported through the appropriate bug-reporting channel and alias. Be sure to adequately describe the problem so that the testers and developers can reproduce it and fix it. See the Release Notes included on the Windows 2000 Beta 3 distribution media for some of the known issues.